IP REPORTS
INNOVATION & FORESIGHT
N°. 08

Scenes from digital life

From problematic situations to legal recourse, an exploration of our day-to-day relationship with data and privacy protection.

LINC
CNIL.

EDITORIAL

Since 2018, the CNIL has observed a "GDPR effect": when people are better informed of their rights, they know how to use them. In the first year of the Regulation's application, the complaints received increased by 33%, then by a further 27% in 2019, before stabilising at around 14,000 complaints in 2020. According to our latest studies, 87% of French people now say they are aware of the issue of data protection and 68% say they are familiar with the CNIL.

This collective awareness is therefore a long-term process and a major strategic challenge for the CNIL, which must organise itself to continue to respond effectively to citizens' demands. The qualitative, sociological and prospective approaches used by its innovation laboratory are essential for getting a better understanding of the processes and the situations in which citizens are led to contact the CNIL, and, *ultimately, for enabling it to strengthen its presence in the digital lives of the French.*

The current law is itself the result of a socio-historical construction that has at its heart the principle of informational self-determination, according to which individuals must be able to control information about themselves, to be informed, and to consent or object to the use of their personal information by others.

Although data protection is based on a common legal foundation, it is approached differently depending on individual values, the social circles to which we belong, the situations we encounter, the resources available to us and the constraints we face. Power relations and socio-economic structural effects can also hamper the effective capacity of individuals to control the flow of information about themselves.

Data protection thus benefits from being considered from the point of view of the plurality of audiences and must be examined taking into account social inequalities and hierarchies. From this perspective, it may be desirable to pay different attention and convey a different message according to the particular vulnerabilities of individuals or social groups.

This Innovation and Foresight report is based on an innovative methodology of sociological analysis of the letters and complaints received. These studies will continue in order to refine our knowledge of the CNIL's audience and their practices, because although data protection is a fundamental right of the individual, it *is a collective right* in a democratic society. The CNIL hopes that the series of recommendations presented in conclusion will achieve this.

Marie-Laure Denis
President of the CNIL

CONTENTS

APRIL 2021
Publication Director:
Louis Dutheillet de Lamothe
and Gwendal Le Grand
Editor-in-Chief:
Bertrand Pailhès
Editors of this report:
Antoine Courmont, Martin Biéri,
Régis Chatellier, with the help
of Pauline Faget, Stéphanie Chapelle
and Ahlam Ammi.

Graphic design:
Agence Linéal
+33 (0)3 20 41 40 76
Printing: DILA
+33 (0)4 71 48 51 05
ISSN: 2263-8881 /
Legal deposit: to be published

The CNIL would like to thank all the members of the Foresight Committee and the external experts who were interviewed or who attended the workshops.

The historical construction of the notions of privacy and personal data protection

"In Rome, there is hardly anything but the debris of public monuments, and these monuments do nothing but trace the political history of past centuries; but in Pompeii, the private lives of the ancients are on display in all their glory."

Madame de Staël, Corinne ou l'Italie (1807)

The historical construction of the notions of privacy and personal data protection

The current law on privacy and personal data protection is the result of a socio-historical construction that emerged in the Western world, in Europe and the United States, as an extension of the "privacy paradigm[1]". Developed in different national contexts and legal traditions, these rights have in common the centrality of the rights of the individual and the principle of informational self-determination.

1 Colin J. Bennett and Charles Raab, *The Governance of Privacy. Policy Instruments in Global Perspective*, MIT Press, 2003

THE EMERGENCE OF A RIGHT TO PRIVACY: THE FOUNDATION OF MODERN SOCIETIES

Gustav Wentzel, Public domain, via Wikimedia Commons

Historians date the emergence of the concept of privacy in around the 18th century with the appearance of specific activities that gradually became independent of public activities. Previously, there was a lot of confusion between public and private, categories that did not really exist[2]. In traditional societies, individuals are enshrined in the community. There is no privacy as such, even if private spaces exist.

> *"[The notion of privacy has been] culturally and historically constructed as a valued and sought-after social value and has been enshrined as a fundamental human right, in a complex movement centred on a private domain embodied first by the family and then by individual space."*[3]
>
> *Bénédicte Rey, 2012*

The distinction between public and private emerged in the modern era. The liberal political tradition was based on the clear distinction between these two spheres that emerged among the urban bourgeoisie in major European cities in the sixteenth and seventeenth centuries. Habermas analysed the birth of public space as a result of the Enlightenment, through the ideal of the 'bourgeois public sphere', a space for free deliberation and rational argument. This approach was materialised in places, lounges, cafés, clubs and other societies where individuals – the cultured bourgeois – would meet to discuss the intellectual works of the time. It is inseparable from modern liberal democracies. This elitist vision is however measured by Arlette Farge, for whom the French public space of the 17th century was not limited to the cultured bourgeois elite but was also composed of the popular masses[4], and does not take into account collective and communal public activities, without being places of public debate, such as festivals, village meetings, etc.

2 Philippe Ariès, *Histoire de la vie privée*, Seuil, 1985
3 Bénédicte Rey, *La vie privée à l'ère du numérique*, Lavoisier, 2012
4 Arlette Farges, *Dire et mal dire, l'opinion publique au XVIIIe siècle*, Seuil, 1992

As a counterpoint, these public spaces presuppose the existence of private, intimate and personal spaces. The private is then defined as opposed to the State, and is understood to be that which escapes it[5]. In the same vein, the French "*cabinet noir*", the violation of the confidentiality of correspondence by the intelligence services, which developed alongside the development of the postal service from the 17th century onwards, was strongly opposed in the 19th century. In this way, privacy is understood as the sanctuary of freedoms by being linked to the public space, which is subject to the gaze of third parties and the control of the authorities. Although initially it only concerned certain social and urban milieus, this retreat into the private sphere gradually became more widespread over the course of the century.

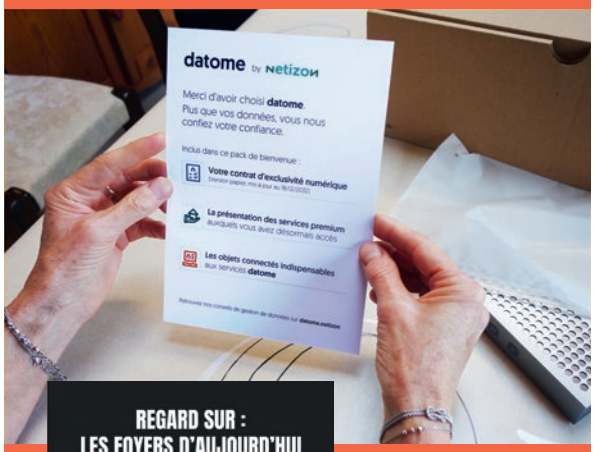
The main private space is that of the family, *"a place of refuge where one escapes the gaze of the outside world, a place of affectivity where sentimental relationships are established between couples and their children[6]"*. It gradually becomes a specific group, distinct from the neighbourhood and extended kinship, which makes the emergence of a form of family privacy possible. This close association between family and private life is materialised in the home. *"The home is a key place to distinguish between public and private. [...] a boundary separating certain types of activities or information. [...] This is only one aspect of the broader process of constructing the notion of privacy, but it is a vital one[7]"*.

A sphere of personal privacy is then gradually built up, which is different from family privacy as there is separation between the martial bedroom and a room intended for the children. This new arrangement of the domestic space meant you could escape the constant gaze of relatives and build *"a personal privacy within the family privacy"*[8]. However, the tendency to have rooms for specific things remained a privilege of the upper classes until the early 1960s and the increasing size of homes, which brought about *"a great novelty, for the people at least: the right of each family member to his or her own privacy. Privacy is thus divided: within the privacy of the family, there is the privacy of individuals[9]"*.

SPECULATIVE FUTURE

Home Sour Home

In the *Home Sour Home* scenario, the future of this private space is questioned by the arrival of connected objects in the home.



REGARD SUR : LES FOYERS D'AUJOURD'HUI

La famille Brillaud vient de souscrire à l'offre datome.

Contre une rémunération mensuelle, la famille s'engage à utiliser exclusivement les services proposés par Netizon. Le géant du numérique s'assure ainsi l'exclusivité de la captation des données de ce foyer.

L'ouverture du pack de bienvenue réserve quelques surprises, avec de nouveaux objets connectés qui s'invitent chez les Brillaud.

Taken from a photo report on 'Today's Homes', the family discovers the *datome* pack after signing a digital exclusivity contract with *Netizon*.

See the off-print: https://linc.cnil.fr/vp2030

5 Philippe Ariès, *Histoire de la vie privée*, Seuil, 1985
6 Philippe Ariès, *Ibid.*
7 Stuart Shapiro, "Places and Spaces: The Historical Interaction of Technology, Home, and Privacy", *in Information Society*, vol. 14, no. 4, p. 275-284, 1998.
Translated and quoted by Bénédicte Rey, *La vie privée à l'ère du numérique*, Lavoisier, 2012
8 Interview with Antoine Prost, "Intime et public: de la construction à la confusion des frontières", *in Sciences Humaines*, 2003/7 (no. 140)
9 Antoine Prost, "Frontières et espaces du privé", in Philippe Ariès and Georges Duby (dir.), *Histoire de la vie privée*, Seuil, 1999

THE CONSTITUTION OF PRIVACY IN LAW

Although they have tended to merge since their inception, the notions of privacy protection (protection de la vie privée) in France and *privacy* in the United States have different origins and approaches. Private sphere protection is thought to have first been recognised in French law rather than US law[10]. Although absent from France's 1789 Declaration of the Rights of Man and of the Citizen, it was mentioned as early as 1791 when the Constitution was revised, and guarantees and limits were introduced on the freedom of the press, particularly with regard to *"slander and insults against any person whatsoever concerning actions in their private lives"*. The notion was taken up in a press law in 1819, and then in the law of 1881 with regard to defamation. In the United States, the notion of *privacy* appeared at the end of the 19th century with a series of lawsuits relating to the use of family names or photographs in advertising without the permission of the data subjects. James Whitman[11] differentiates between the European and American visions according to two approaches: dignity and freedom. The European tradition is concerned with the protection of dignity, in line with the notion of honour of the Ancien Régime, while the American tradition is focused on freedoms from the state – the facts show that the two approaches coexist on both sides of the Atlantic.

Since the modern era, the rise of privacy protection as a fundamental private right is inseparable from the rise of individualism in our societies. It is also linked to the evolution of technology, which adapts its framework and prevents substantial content from being established. Printing, photography and the resulting disclosure of private information led to the first formalisation of the right to data protection – *privacy* – by the American lawyers Warren and Brandeis in 1890. The article they published constitutes the birth of the right to privacy in its Anglo-Saxon conception and is part of a liberal and bourgeois conception of society. This first dialectic between law and technology already illustrates the impact of the latter on the perception of privacy: by recording, disseminating and storing information or events that would otherwise remain solely in the memory of the participants, technology blurs the lines between private, confidential life and public activities known to others.

Warren and Brandeis formalised this new right, which they defined as *"the right to be left alone"*. This right to privacy as a principle of non-intrusion is the basis of privacy

Focus on...

A typology of the meanings and values of privacy

The *Stanford Encyclopedia of Philosophy Archive* offers a typology of the values associated with protection of privacy:

- **Control over information:** when, how, and to what extent information about us is communicated to others (Westin, 1967).
- **Human dignity:** or the inviolate personality, defining one's essence as a human being (dignity, integrity, personal autonomy and independence) (Bloustein, 1964).
- **Intimacy:** control over information about oneself, which allows one to maintain varying degrees of intimacy in love, friendship and trust relationships (Fried, 1970).
- **Social relationships:** allows one to develop diverse interpersonal relationships with others, to protect one's assets or interests, or to protect one from embarrassment, or to protect one against the deleterious consequences of information leaks (Rachels, 1975).
- **Restricted access:** physical access, to personal information or attention, through anonymity (Gavison, 1980), to which physical access to one's body can be added (Moore, 2003).

DeCew, Judith, "Privacy", *The Stanford Encyclopedia of Philosophy* (Spring 2018 Edition), Edward N. Zalta (ed.), https://plato.stanford.edu/archives/spr2018/entries/privacy/

10 Jean-Louis Halpérin, "Protection de la vie privée et privacy : deux traditions juridiques différentes ?", *Les Nouveaux Cahiers du Conseil constitutionnel*, vol. 48, no. 3, 2015, pp. 59-68.
11 James Whitman, "The Two Western Cultures of Privacy: Dignity v. Liberty", *The Yale Law Journal*, 2004, 113, p. 1151-1221.

protection legislation. For example, the 1948 Universal Declaration of Human Rights states in Article 12: *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to protection from the law against such interference or attacks"*. The legal arsenal of privacy protection defines privacy in contrast to the notion of intrusion. As Bénédicte Rey points out, *"privacy has become a fortress to be defended, to the benefit of an individual who is in an unequal power relationship with possible intruders"*[12]. Protection of the private domain is built against intrusions emanating mainly from the government and mass media.

> *"Privacy is the control we have over information about ourselves."*
>
> *Charles Fried, Privacy, 1968*

In this liberal paradigm, the right to privacy is seen as a fundamental right necessary for the exercise of other fundamental rights and freedoms in our democratic regimes: freedom of opinion, freedom of movement and assembly, freedom of association, political and religious freedom, free choice of morals and social relations, etc. At an individual level, privacy is essential for self-determination, self-construction and the cultivation of individuality[13].

Over the course of the 20th century, this liberal conception of privacy based on restricting access to the private sphere was gradually enriched to defend the individual's control of information concerning him or her, as shown by the definitions given by the American lawyers Alan Westin, Charles Fried and Arthur Miller in the 1960s.

Thus, the individual must be able to control the information about him or her, and to consent to or object to the use of his or her personal information by others. This right to informational self-determination was to form the basis of the personal data protection legislation developed in Western countries from the 1960s onwards.

PROTECTION OF PERSONAL DATA: A RIGHT TO INFORMATIONAL SELF-DETERMINATION

Thus, a right to protection of personal data emerged in Western countries. While it was a continuation of the right to protection of privacy, it broadened it to take into account the relationship between IT and society. Rather than being limited to the effects of IT on privacy, this new legislative framework would question public and individual liberties with regard to the development of this technology. The right to protection of personal data responded to the concerns linked to the development of information technology and databases on the freedom and autonomy of individuals and was expected to restore the confidence – of the citizen and the consumer – in information technology.

It was a time of large *mainframes*, the product of the needs of the Cold War military-industrial complex and rapidly used for a variety of applications. Far from the Californian utopia of the 1970s, which associated the computer with emancipation[14], computers were perceived as a danger and a threat to individuals. Two works of science fiction, very popular at the time, illustrated this feeling: *1984* by George Orwell (published in 1949) and *2001, A Space Odyssey* by Stanley Kubrick (1968). They helped to transform the image of the computer, which was no longer considered only as a tool for automating laborious mathematical tasks, but as a bureaucratic machine for the rationalised control of the population – or of a crew.

In Western countries, a coalition of stakeholders, mainly made up of senior civil servants, would formalise the principles – still largely in force – on which national personal data protection laws would be based. This frame of reference, which some authors call the "privacy paradigm"[15], is part of the liberal perspective of the right to informational self-determination (the free disposal of one's personal data). Rather than actually defining what belongs to the public or private sphere, it implies leaving the individual free to decide on the circulation of his or her personal data, by endowing him or her with a set of technical rights[16]. Personal data is not only data relating to the privacy of individuals, but any information that can, directly or indirectly, identify an individual. Thus, as the Court of Justice of the European Union reiterated: *"the notions of personal data [...] and data relating to privacy are not the same thing"*[17]. Therefore, while the spheres of personal data protection and protection of privacy may overlap, they each have their own specificities.

12 Bénédicte Rey, "Vers un changement de perspective pour garantir le droit à la vie privée ?", *Les Cahiers du numérique* 2014/1 (Vol. 10), pages 9 to 18
13 Judith Wagner DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, Cornell University Press, 1997
14 Fred Turner, *Aux sources de l'utopie numérique : De la contre-culture à la cyberculture, Stewart Brand, un homme d'influence*, C&F Editions, 2012
15 Colin J. Bennett and Charles Raab, *The Governance of Privacy. Policy Instruments in Global Perspective*, MIT Press, 2003

Focus on...

Protection of privacy or protection of data?

Often used interchangeably, personal data protection and protection of privacy have distinct legal frameworks and differ in scope. While in France, the case law of the Constitutional Council has not separated the protection of personal data from privacy protection, in Europe the Charter of Fundamental Rights of the European Union separates the two notions: Article 7 enshrines respect for private life, while Article 8 raises the protection of personal data as a fundamental right.

The notion of privacy is more related to the privacy of individuals, whereas data protection is broader, and includes privacy. It should be noted that the only occurrence of the term "private life" in the General Data Protection Regulation (GDPR) is in Recital 4, which itself refers to the Charter of Fundamental Rights. The term *privacy* does not appear in the English version, only "*private and family life*". On the other hand, it can be found in the e-Privacy Directive (Directive on privacy and electronic communications) relating to the confidentiality of communications, which overlaps with the GDPR in its application[18].

In practical terms, the right to the protection of personal data results in a "number of technical rights" (information, access, rectification, erasure and portability), whereas the right to privacy involves identifying what constitutes privacy[19]. While the emergence and development of digital technology initially led us to believe that the protection of personal data should be the subject of an autonomous law, the massification of data – the granularity of which is becoming ever finer – has led some authors, such as Antoinette Rouvroy[20], to call for a strengthening of the links between data and private life. In practice, application of the GDPR and the French Data Protection Act allows this. Data protection reinforces the protection of the right to privacy to ensure its effectiveness.

Thus, data that is not directly private, or even public data or data shared publicly by individuals, remains data subject to data protection. It is protected because of its personal nature and its use could breach human identity, human rights, privacy, or individual or public liberties, according to the terms of Article 1 of the French Data Protection Act.

Thus, data protection is intended to protect private life, but sometimes also public life.

16 Such as the right to information, the right of access, the right to rectification, the right to object, the right not to be subject to an algorithmic decision, the right to be delisted and the right to erasure.
17 CJEU, 16 July 2015, "ClienthEarth" Case. C-615/13 P pt. 32, cited by Julien Rossi and Jean-Édouard Bigot. "Traces numériques et recherche scientifique au prisme du droit des données personnelles",
Les Enjeux de l'information et de la communication, vol. 19/2, no. 2, 2018, pp. 161-177.
18 https://www.cnil.fr/fr/cookies-et-autres-traceurs-la-cnil-publie-des-lignes-directrices-modificatives-et-sa-recommandation
19 Audrey Bachert-Peretti, "La protection constitutionnelle des données personnelles : les limites de l'office du Conseil constitutionnel face à la révolution numérique", *Revue française de droit constitutionnel*, 2019/2 (no. 118), p. 261-284
20 Antoinette Rouvroy, "Homo juridicus est-il soluble dans les données ?", *Droit, normes et libertés dans le cybermonde*, Liber Amicorum Yves Poullet, Larcier 2016

Focus on...

Critics of the liberal privacy paradigm

The liberal privacy paradigm is now widely accepted, especially by the digital economy industry, which negotiates the application of its main principles rather than questioning them. However, it has been the subject of criticism from various quarters[21].

Economists from the Chicago School of Economics have been opposed to any form of regulation of personal data since the 1970s. They perceive the right to privacy as an obstacle to the optimal functioning of markets, insofar as it constrains the condition of transparency of information. Furthermore, feminist criticism denounced the binary opposition between public space and private sphere, which prevents the publicising of what is considered private, such as domestic violence, which has long been relegated to the private sphere, limiting its politicisation.

Christian Fuchs also criticises the 'fetishism' of privacy and the blindness of the individualistic conception of the liberal paradigm to relations of class and gender domination. According to him, *"capitalism protects privacy for the rich and companies, but at the same time legitimises privacy violations of consumers and citizens"*[22].

Finally, the Marxist approach analyses the collection of personal data in relation to the development of informational capitalism. From this perspective, individuals are caught in an exploitative relationship through which they not only suffer intrusion into their private sphere, but also alienation into a form of data-producing labour. To counter this, they believe it is necessary to create a collective balance of power and to consider the protection of personal data through the regime of the commons[23].

21 Julien Rossi, *Protection des données personnelles et droit à la vie privée : enquête sur la notion controversée de "donnée à caractère personnel"*, Doctoral Thesis, information and communication sciences, Université de Technologie de Compiègne, 2020
22 Christian Fuchs, "Towards an alternative concept of privacy", *Journal of Information, Communication and Ethics in Society*, vol. 9, no. 4, p. 220-237
23 Laura Aufrère and Lionel Maurel, "Pour une protection sociale des données personnelles", 2018 https://scinfolex.com/2018/02/05/pour-une-protection-sociale-des-donnees-personnelles
24 http://www.le-tigre.net/marc-l.html

Diversity of data protection practices and behaviours

"Happy birthday, Marc. On 5 December 2008, you will be celebrating your twenty-ninth birthday. Do you mind if we speak informally, Marc? You don't know me, that's true. But I know you very well. You are (un)lucky to have been chosen as the first Google portrait from Le Tigre. It's quite simple: we take an anonymous person and tell his or her life story using all the traces he or she has left, deliberately or otherwise, on the Internet. (...) I should probably warn you: it will be shameless, the opposite of everything we stand for at Le Tigre."

In 2008, the Le Tigre newspaper[24] drew a portrait of an unknown person based on traces freely accessible on the Internet, to make the point that, once collected, scattered and seemingly insignificant *information* can provide a detailed description of an individual's life.

Diversity of data protection practices and behaviours

Our digital practices are deeply social.
They are embedded in power relations and enshrined in socio-economic structures, which hinder the effective capacity of individuals to control the flow of information concerning them.

FROM INTRUSION TO SELF-EXPOSURE: THE DIVERSITY OF DIGITAL AND PERSONAL DATA PROTECTION PRACTICES

Pexels cc-by Aleksandar Pasaric

The end of privacy?

Faced with the rise in the collection of traces of individuals' actions and preferences by commercial firms and their exposure on social networks, several authors have pronounced an "end to privacy". Mark Zuckerberg or Eric Schmidt argued in the early 2010s that privacy was an obsolete concept. These opinions, which justify their own commercial choices of using their users' traces, are nevertheless in contradiction with the practices of individuals. Expressing oneself in a public online space, or any act of self-exposure, is not incompatible with the desire to have and the fact of having privacy.

Empirical surveys of digital practices contradict these claims as argued by sociologists Alice Marwick and danah boyd: *"People care deeply about privacy and develop innovative strategies to achieve privacy while participating in the systems that allow them to access information, socialize with friends, and interact with contemporary entertainment platforms"*[25]. Individuals develop strategies to control what information they wish to disseminate and to whom, ensuring how it is received and interpreted. However, they do not hold all the cards when it comes to controlling these information flows, which are largely embedded in socio-economic structures over which they have little control. As the sociologist Antonio Casilli analyses, privacy is negotiated, on a case-by-case basis, depending on the situation[26].

25 Alice E. Marwick, danah boyd, "Understanding Privacy at the Margins", *International Journal of Communication*, 12(2018), 1157–1165
26 Antonio A. Casilli, "Contre l'hypothèse de la 'fin de la vie privée'", *Revue française des sciences de l'information et de la communication*, 3, 2013

SPECULATIVE FUTURE

Home Sour Home

This scenario explores the new practices of disclosure and control of your data in 2032.

REGARD SUR : LES FOYERS D'AUJOURD'HUI

Marion et Théo sont adeptes du Grand Oubli. Tous les jours, à 22h, ils se connectent à leurs gestionnaires de données respectifs.

Le rituel est immuable, chacun est installé dans son coin et passe en revue les données produites au cours de la journée.

Sans concertation et dans un silence total, Marion et Théo décident lesquelles de leurs données personnelles sont effacées ou conservées.

Taken from a report on "Today's Homes", with a couple who use the "Grand Oubli" service.

https://linc.cnil.fr/vp2030

There is a large body of academic work on the practice of self-exposure on social networks[27]. It highlights the fact that individuals make strategic use of the disclosure of personal information to construct an identity (online or offline) and social capital. However, the visibility of individuals depends on their know-how, their mastery of the tool and their understanding of its norms. There is therefore an inequality that separates the uninitiated from the initiated. The desire to control one's image also varies according to the social characteristics of individuals. For example, several studies on the digital uses of teenagers have shown that it is more important for young girls than for boys[28], and above all that it is more complex and difficult for women to control their visibility online[29]. These studies also point out that reflexivity about digital practices increases with age. Dominique Pasquier notes that the search for online recognition is not at the heart of the digital practices of the working classes, whose "participatory modesty" leads them to favour exchanges with their close friends and family[30].

Finally, the capacity to implement these strategies for negotiating one's privacy is unequal among individuals. On the one hand, this requires technical skills in the operating principles of the systems used on a daily basis; on the other hand, it involves mastering the codes of different social environments. It is often difficult to understand what the norm may be in a given situation. Benjamin Bitane, head of training at Emmaüs Connect, notes this problem among certain young people who use digital technology recreationally, but have a difficult relationship with other subjects. *"They are now in control of their image on social networks in relation to their daily life and peer group. But what they don't grasp at all is the porous nature of their image, when it changes social world. It's hard to get them to understand that the mailbox bg75@coucou.fr is not appropriate, or that their future employer may come across the video on YouTube where they are drunk with their mates. So, while they are very comfortable on social media, they do not at all have the 'serious' digital habits and customs, the traditional codes"*[31]. These situations of 'context collapse'[32], where our social spheres collide, are not unique to the digital world, but have become more pronounced with social networks. However, the ability to manage multiple self-representations and to navigate between social worlds is unevenly developed among individuals. Juggling different environments and identities requires specific skills and perspective, an understanding of community norms and practices, and the ability to present ourselves consistently in the different environments in which we interact. This difficulty is further compounded by the networked nature of the digital environment: *"Contexts do not collapse by chance; they dissolve because individuals have different conceptions of the existence of boundaries and of how their decisions affect others"*[33]. Each person may have a clear vision of what is appropriate in a particular situation, but their friends may not share their understanding of these social norms.

27 See in particular, Dominique Cardon, "Le design de la visibilité. Un essai de cartographie du web 2.0", *Réseaux*, 2008/6 (no. 152), p. 93-137.

28 See in particular: Céline Metton-Gayon. Les adolescents, leur téléphone et Internet. "Tu viens sur MSN ?" Paris: L'Harmattan, 2009, 202 p & Bruna, Yann. "Snapchat à l'adolescence. Entre adhésion et résistances", *Réseaux*, vol. 222, no. 4, 2020, pp. 139-164.

29 Alice Marwick, (2013) "Gender, Sexuality and Social Media." In Senft, T. & Hunsinger, J. (eds), *The Social Media Handbook*. Routledge, 2013, pp. 59-75.

30 Dominique Pasquier, *L'Internet des familles modestes. Enquête dans la France rurale*, Presses des Mines, 2018, 222 p

31 In an interview with LINC, 12 March 2020

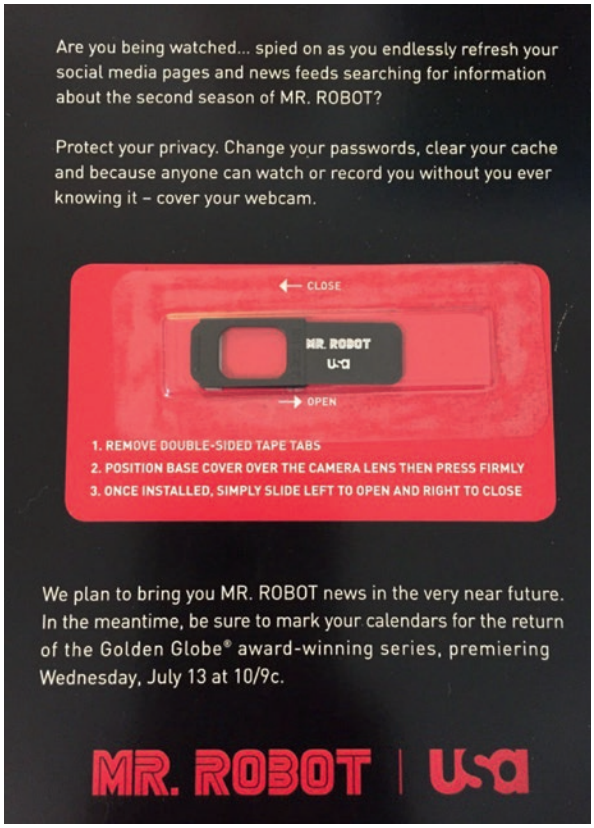
32 danah boyd, *It's Complicated: The Social Lives of Networked Teens*, C & F éditions, 2016

33 danah boyd, *Ibid.*, p. 118

Daily data protection practice

Beyond the dynamics of expression on social networks, people exploit the cracks and blind spots of surveillance infrastructures and practices to forge their own spaces, protect their privacy, get a bit of respite, and play around with what they wish to hide or reveal. Although they are not technical experts, they are creative in dealing with socio-technical devices to protect their privacy. In the shadow of legitimate knowledge, they implement tactics and develop lay skills to protect their personal data, which may or may not be close to the recommended norms, and based on practical knowledge rather than on technical or legal knowledge. In this respect, individuals are very creative in protecting their privacy and their data: a bit of tape stuck over their webcam, cases knocked up to avoid contactless payment fraud, installation of an ad blocker, provision of false information in online forms, multiple or shared accounts, use of pseudonyms, use of several email addresses for different uses, registration on a Do No call list, regular deletion of cookies, etc. While the effectiveness of these techniques varies, they are indicative of a discomfort and fear of unauthorised data collection. This proliferation of self-protection strategies is, moreover, made particularly necessary by the very great uniformity of digital service offerings: because of the global nature of the companies that offer them and the economies of scale they provide, they are designed on a single model for the whole world, generally derived from the needs and expectations of the US market. The lack of regional or national specificity and the impossibility of customising processes and services or having access to an alternative leads individuals to bypass or divert what is in their hands (hardware, the fields of a form, etc.).

> *"When you ask a teenager: "Can I see your account?", he replies "which one?". Usually he has two or three. There's the one for his parents, the one for school and the one for his friends. All with very different identities. It shows not only an awareness of the consequences of their online image, but also a reflexivity and an ability to act."*
>
> *Anne Cordier*[34]



From post-it notes to promotional webcam covers: everyday practices to protect your privacy.

34 Xavier de la Porte, interview with Anne Cordier, Sommes-nous en train de fabriquer des « crétins digitaux » ?, *Podcast: Le code a changé*, France Inter, https://www.franceinter.fr/emissions/le-code-a-change/sommes-nous-vraiment-en-train-de-fabriquer-des-cretins-digitaux

Digital practices anchored in social relations

While they are often accused of unwittingly revealing themselves, work on the digital practices of the adolescent population shows a reflexivity and an understanding of the economic model of the services they use. We need to rid ourselves of the preconceived ideas that young people, the less educated or the more frail are less vigilant about privacy and are lax or negligent in protecting their personal information. These moralising discourses reduce the problem to an individual dimension and tend to obscure the conditions that favour the dissemination of personal information in the daily practices of individuals. This moral, even paternalistic, focus on individual behaviour overlooks the fact that protecting one's privacy and personal data is not always, or is rarely, a simple individual decision, but a complex trade-off in what can be difficult social conditions.

> *"If you want to escape the collection of your data, you are marginalised."*
>
> *Cristina Machado* [35]

Individuals are in fact inserted into social relationships that determine their use of digital technology. For example, exercising your social rights requires you to have an email address and to disclose information. Stéphane Koukoui, digital mediator in Rennes, testifies: *"It is difficult to escape the pressure of Big Tech. You go to a community centre, you say that you don't have email and that you would like one to set up your (employment office) account. They will open a Gmail account for you*[36]*"*. Another example, as anthropologist Pascal Plantard points out, integrating into a social group may require the use of social networks: *"adolescent socialisations no longer distinguish between ordinary social norms and digital social norms. Social networks have become spaces where you talk to your friends, just like at school or on the football pitch. Teens need it so that they do not feel excluded from the group and so that they can talk to each other, away from the gaze of their parents*[37]".

Working for a company or an organisation can also lead to the imposition of tools whose principles one does not share, even when one is used to being very vigilant, like Antonio Casilli: *"[with lockdown] I think that what has been going on for the last 15 years has been played out. We don't give up our privacy, but we choose the battles we can win. On the other hand, in some cases, strategic retreats are required. I am thinking of the use of certain tools such as Zoom. [...] Personally, it was my employer who offered it to me. Either that or there is no communication. You can compromise, you can put in place strategies to limit the damage, for example choosing the equipment that connects or choosing the place from where you connect and so on. But there are times when it is difficult to do otherwise*[38]".

Our digital practices are thus embedded in social relations and socio-economic structures. It is difficult for an individual to adopt data-saving practices when the whole economy seems to be about capturing as much data as possible about the individual. The incentives to reveal oneself are constant and the network effects, which reinforce the concentration of activities on a few tools, make it particularly difficult to withdraw from collective dynamics. Above all, as digital technologies have penetrated all of our environments, we inhabit the digital world even when our practices do not: walking down the street today inevitably means leaving a certain number of traces. Not being on a social network does not mean that we do not have a digital existence.

In 2019, journalist Kashmir Hill tried the experiment of going without Big Tech for several weeks[39]. This proved particularly difficult as these companies are the infrastructure on which a large part of digital services are based. For example, cutting yourself off from Amazon means losing access to all sites hosted by Amazon Web Services, the leading cloud provider. Denying Google access means denying access to all sites and applications that use the company's services to display advertising, publish a Google Maps map, track their users, or determine whether visitors are humans or robots. She concludes: "*After the experiment was over, though, I went back to using the companies' services again, because as it demonstrated, I didn't really have any other choice*[40]". Therefore, rather than a *'privacy paradox*[41]', which implies freedom of choice, individuals are resigned to the absence of concrete means of exercising an action on the circulation of their data[42].

35 In an interview with LINC, 13 October 2020
36 Cited by https://labs.letemps.ch/interactive/2020/longread-donnees-personnelles/
37 https://www.liberation.fr/debats/2020/09/10/pour-les-collegiens-etre-populaire-peut-etre-lie-a-avoir-des-flammes-sur-snapchat_1799108
38 Xavier de la Porte, interview with Antonio Casilli, COVID, confinement et grande conversion numérique, with Antonio Casilli, *Podcast: Le code a changé*, France Inter https://www.franceinter.fr/emissions/le-code-a-change/covid-confinement-et-grande-conversion-numerique-avec-antonio-casilli
39 Kashmir Hill, "I Cut the 'Big Five' Tech Giants From My Life. It Was Hell", *Gizmodo*, July 2019, https://gizmodo.com/i-cut-the-big-five-tech-giants-from-my-life-it-was-hel-1831304194
40 Kashmir Hill, "I Tried to Live Without the Tech Giants. It Was Impossible.", *New-York Times*, July 2020 https://www.nytimes.com/2020/07/31/technology/blocking-the-tech-giants.html
41 The *'privacy paradox'* is the contradiction between the concern individuals say they have about the collection of their personal data and their actual information sharing practices.
42 Draper, N. A. and Turow, J. (2019) "The corporate cultivation of digital resignation", *New Media & Society*, 21(8), pp. 1824–1839

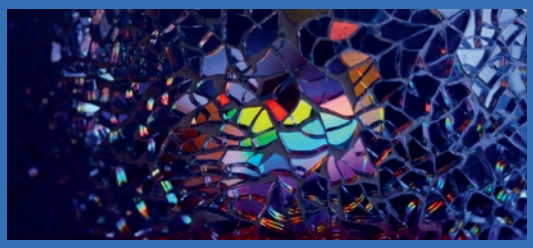
Better equipped, but more collected

Sociologists danah boyd and Alice Marwick emphasise to what extent protection of privacy is a daily struggle, from which certain populations, those involved in unfavourable power relations, rarely emerge victorious[43]. With the ever-increasing digitalisation of our societies, the ability to *opt out* of automated systems is becoming more and more of a privilege. While for some the collection of data is consented to, for others it is imposed. Because they have less power to resist it, certain social groups are more targeted by intrusive programmes.

The example of the use of social rights illustrates the constraints on individuals' control of their information. Beneficiaries have no choice but to enter into a regime of transparency regarding their practices in order to make use of their social rights. As Héléna Revil, a political scientist at the Observatoire des non-recours aux droits et services (ODENORE), explains: *"To use one's rights is, in a way, to be seen, to make oneself visible. In order to access certain benefits, aid and services, based on different criteria, a large number of supporting documents must be provided. People may feel exposed. When you are not in a vulnerable situation, you don't realise that you need to expose yourself*[44]". In the fight against social benefit fraud, this intrusion into the private sphere of individuals is increasing, without users always being aware of the transfer of their data to other departments, as the ***Défenseur des Droits*** (Defender of Rights) laments. *"It should be noted that the procedures for use of inter-agency cooperation and the right of communication mentioned in CAF (family benefits) or MSA (farmer's mutual plan) application forms only appear at the bottom of the page, in the small print, even though these control procedures are the counterpart of the payment of the benefit*[45]". In addition to the administrative data that is gradually being shared between social bodies, this transparency requirement is tending to extend to more and more aspects of daily life. The introduction of a "right of communication" gives officials in charge of control in organisations – extended to Pôle Emploi (employment office) officials with the 2021 French Finance Bill[46] – the power to request various documents from banking institutions, telephone operators or energy suppliers. Some authorities even go beyond their authorisations, as denounced by the *Défenseur des Droits*. *"Some departmental councils have also demanded the production of beneficiaries' car, motorbike and home insurance certificates. These documents serve no purpose for checking the conditions of eligibility or calculating the amount of the earned income supplement, but they do make it possible to assess the recipient's lifestyle*[47]".

For the American legal expert Michele E. Gilman, the most vulnerable populations are required to exchange their privacy for access to social rights. She concludes that poor Americans experience privacy differently from people with greater economic resources. There are social class differences in the right to privacy[48].

FRAGMENT OF IMAGINATION



"Telling the story of two successive experiences during which the artist Mark Farid first practically disappeared from the digital world and then reappeared, making all his digital traces public, including of course those concerning his interactions with third parties. His conclusion: it is much harder to be invisible than to be overexposed, including from a psychological point of view. But he links this to the way in which the digital world has organised itself and organises the world: many of life's functions are no longer accessible outside of the digital, and public exposure steers our practices in directions that we know are socially rewarding, creating a form of satisfaction devoid of any reflexivity. For Farid, it is true that we cannot "live" today without giving up our data to digital platforms, but this makes political choices all the more necessary: the individual level is not the right level to reconstitute room for manoeuvre."

See the off-print: https://linc.cnil.fr/vp2030

43 Alice E. Marwick, danah boyd, "Understanding Privacy at the Margins", *International Journal of Communication*, 12(2018), 1157–1165

44 In an interview with LINC (24 November 2020)

45 Report *Lutte contre la fraude aux prestations sociales : à quel prix pour les droits des usagers ?*, Défenseur des droits, 2017, p. 20

46 Bertrand Bissuel, "Pôle emploi obtient de nouveaux pouvoirs pour combattre la fraude", *Le Monde*, December 2020, https://www.lemonde.fr/politique/article/2020/12/19/pole-emploi-obtientde-nouveaux-pouvoirs-pour-combattre-la-fraude_6063941_823448.html

47 Report *Lutte contre la fraude aux prestations sociales : à quel prix pour les droits des usagers ?*, Défenseur des droits, 2017, p. 24

48 Michele E. Gilman, "The Class Differential in Privacy Law". Brooklyn *Law Review*, Vol. 77, No. 4, Summer 2012, Available at SSRN: https://ssrn.com/abstract=2182773

OFF-PRINT

From the fragment of imagination to the speculative artefact, fictions for exploring the future

Alongside this Innovation and Foresight report, we are publishing an off-print online that aims to trace the different futures of privacy up to 2030. A prospective and speculative exploration carried out on the initiative of LINC, supported by the studios Casus Ludi / Design Friction, Chronos and Daniel Kaplan, as well as experts in all fields.

This exploration aims to propose new narratives and imaginations that allow us to question the protection of personal data in 2030 and to bring a reflexivity to regulation practices.

Throughout the process, we sought to highlight the frictions that could be triggered by the use of technologies in different social groups and at different moments of digital life, as well as the risks that would arise for individual and collective liberties.

Three complementary approaches are deployed – imaginations, speculative fiction and design fiction – to explore four complementary and intersecting areas: everyday life, ordinary digital practices, social inequality and differentiation, and the relationship to privacy.

This 80-page document transcribes these explorations, including an "analysis of fictional and artistic fragments" collected following a call to Internet users in August 2020, and "three speculative futures for privacy up to 2030": Reputable or repudiated, Managing the unmanageable, Home Sour Home.

You can find extracts of it in this report, in the form of boxes, and browse this exploration online.

Download the off-print: https://linc.cnil.fr/vp2030

WHY DO WE BEHAVE DIFFERENTLY WHEN IT COMES TO PROTECTING OUR DATA?

The protection of personal data, and in particular the GDPR, aims to ensure that the fundamental rights of each individual are respected. To this end, it attributes rights to individuals and obligations to data controllers and processors, i.e. companies and any organisations that collect and process data. Individuals thus have rights, including the right to use services based on the collection of their data, and above all the right to change their mind. It is up to the companies to allow them to do so. Ultimate responsibility always lies with the data controller. However, the harm caused to individuals by mismanagement of their data, and of their image, can have negative consequences, which often fall outside the scope of data protection law, especially in relation to privacy, and social media for example. For these reasons, data protection goes hand in hand with a policy of prevention for individuals in order to limit the risk of becoming a victim.

This preventive policy with regard to data protection is based in particular on the ability to implement appropriate measures to guard against malicious practices. To this end, a set of prescriptions aims to make individuals more forward-looking and to adopt a "risk culture" with regard to their personal data, i.e. to anticipate the future consequences of their individual practices. For some, this may take the form of foresight orders, sometimes through moral condemnation of behaviour deemed reckless, for example with the stigmatisation of teenage practices on social media (page 18). But this can correspond to more positive and productive ways of relying on 'good practices' in relation to privacy and personal data protection. While individuals are developing lay data protection skills, digital training schemes[49] – from schoolchildren to people far removed from the digital world – aim to make these individuals internalise new digital practices that will enable them to avoid certain pitfalls: creating a secure password, setting up their browser and digital service accounts, managing their consents closely, controlling their online identity, using a pseudonym, etc.
While many people apply these prevention standards, their implementation remains difficult. It is not enough to get the message across for people to easily adopt the 'right' practices and behaviours. Not all individuals are exposed to the prevention message in the same way, the conditions for receiving it differ, and finally, not everyone is equal in applying it. Work carried out in the fields of health, the environment, food or road safety highlights the fact that messages are received in different ways depending on social context, lifestyle and the material and symbolic resources of individuals[50]. Although the principle of foresight is universal, having foresight is the subject of unevenly distributed provisions[51]. It can be assumed that these results apply in the case of personal data protection, and should be taken into account when supporting people.

Preventive policies and normative tensions

Preventive policies, especially if they are based on a form of stigmatisation, involve a degree of symbolic violence when they encourage individuals to change their practices without taking into consideration the norms and values on which these practices are based. Implementing the right ways to protect personal data involves conflicting values and interests that are often neither clearly stated nor discussed. In a situation, data protection can rarely be isolated from other considerations. Individuals are confronted with multiple micro-decisions that they have to make without the risk to their privacy always being prioritised over the different social norms that weigh on them. Indeed, tension can arise between this objective and other imperatives and interests at stake in the different spheres of their lives (work, friends, family or public life). For example, normative tensions between the concern to protect privacy and the risk of provoking conflict with one's employer or jeopardising family harmony will most often lead to the latter being favoured over the former. As the sociologist Amitai Etzioni summarises, *"Privacy has to find its place among a whole set of values that we hold dear and that are not always entirely compatible. Therefore, we should always weigh up the importance we are prepared to give to privacy against the importance we are prepared to give to other values, especially the protection of our families, our communities and our homeland[52]".*

As the sociologist Dominique Pasquier points out, these normative dissonances are particularly visible among the working classes she has studied. *"There is a tension between working class familialism and the individual nature of the tools (phone, email address, password, etc.) that challenges working class values. In my survey, the family collective*

49 See, for example, the recommendations available on the CNIL website (https://www.cnil.fr/fr/maitriser-mes-donnees) or the sheets for trainers designed by Les Bons Clics (https://www.lesbonsclics.fr)

50 Benoît Bastard, "Quel sens donner aux comportements à risque face au Covid-19 ?", *AOC*, 5 June 2020, https://aoc.media/analyse/2020/06/04/quel-sens-donner-aux-comportements-a-risque-face-au-covid-19/

51 Jean-Baptiste Comby, Matthieu Grossetête, "Se montrer prévoyant: une norme sociale diversement appropriée", *Sociologie*, 2012/3 (Vol. 3), p. 251-266. https://www.cairn.info/revue-sociologie-2012-3-page-251.htm

prevails over individual life, there are attempts to make the tools less individualised. People swap phones. Couples, or even whole families, share the same email address and we are systematically "friends" on Facebook. Sharing passwords is a principle of collective life. Not giving out the password to your account or phone will be seen as a sign of deception or concealment. This is not right[54]*".* While it invites further investigation into the specificities of the relationship to personal information according to social background, this observation illustrates that the issue of data protection cannot be considered only from an individual perspective. Individuals are inserted in a family or friendship setting whose values and expectations may lead them to share a password or give access to their Facebook or SnapChat account to prove their loyalty and trust[55]. In the face of other values and imperatives, the boundaries of privacy can thus be restricted.

> *"It's very hard [to implement data protection practices] because our digital practices are so ingrained. For some people, simply changing their webmail icon is very complicated. It is a real assault to change our habits"*[53]
>
> *Pierre-André Souville, digital mediator, Rennes*

In addition, the solutions proposed may be considered restrictive and difficult to implement. The "right" practices can disrupt routine digital use. This can lead to a distancing from these privacy protection norms: critical discourse, rejection of certain services deemed too restrictive, maintenance of alternative practices, playing with the recommendations to adapt them to their world of professional or family constraints, arrangements with the norm, etc. The causal link between knowledge of data protection principles and the implementation of practices that comply with them must therefore be moderated. We know that without secure passwords, we are at risk of having our digital accounts hacked. However, it is difficult for many of us to implement this recommendation. For example, the difficulties in remembering complex and multiple passwords lead us to favour the simplicity of similar passwords that are easier to remember or to record them in a "password book" which, if lost or revealed to a third party, can be harmful. This behaviour is not irrational. On the contrary, we all have good reasons for not adopting data protection standards. For prevention messages to be as relevant as possible, it is necessary to understand these reasons and the meaning we give to these practices.

Data protection socialization

The social groups we belong to play a central role in the individual socialisation to the protection of our personal data. On the one hand, our values are strongly influenced by existing family socialisation (see above). On the other hand, integration into family, professional, political or friendship networks gives access to resources, to 'IT capital'[56], and significantly changes data protection practices. The longitudinal work carried out by the sociologist Anne Cordier, who follows young people over several years, shows that the evolution of their strategies and practices in terms of personal data protection is closely linked to their integration into different circles of sociability[57]. For example, a young female activist in an anti-fascist movement has radically transformed her data protection practices. Individuals thus adapt to the

FRAGMENT OF IMAGINATION

"The Uninvited Guest scenario, by the studio Superflux, shows an elderly person forced to come up with ploys to live the life he has chosen despite the orders of the many connected objects his (loving) family has forced on him."

See the off-print: https://linc.cnil.fr/vp2030

52 Amitai Etzioni, *The limits of privacy*, Basic Books, 1999, p. 260
53 In an exchange with LINC, 1 October 2020
54 LINC.cnil.fr, interview with Dominique Pasquier, "*Dans les classes populaires, la vie privée relève moins de l'individu que du groupe familial*", March 2020 https://linc.cnil.fr/fr/dominique-pasquier-dans-les-classes-populaires-la-vie-privee-releve-moins-de-lindividu-que-du-groupe
55 Margot Déage, "S'exposer sur un réseau fantôme. Snapchat et la réputation des collégiens en milieu populaire", *Réseaux*, 2018/2-3 (no. 208-209), p. 147-172.
56 Cédric Fluckiger, "Les collégiens et la transmission familiale d'un capital informatique", *Agora débats/jeunesses*, 2007/4 (no. 46), p. 32-42
57 Anne Cordier, "Du design de la transparence à l'agir informationnel : Les apports d'une approche sociale de l'information", 2017

social norms expected by a social environment. Similarly, practices imposed in the workplace can lead to the transfer of skills into personal practices.

Those close to us play a crucial role in learning about data protection practices through mutual support and the sharing of good practices. Irène Bastard notes that older siblings supervise teenagers' first steps on Facebook and transmit generational codes and practices to them[58]. Pierre-André Souville, digital mediator in Rennes, confirms: *"learning is very much a peer process. Words are more meaningful when they come from the people around us. Children, friends, neighbours or colleagues are the first ones people turn to when they have a problem with the digital world[59]"*. The Capacity survey also showed that the key factor in digital exclusion is not social class but isolation, as the coordinator of this research project, Jacques-François Marchandise, points out: *"Socialised people do much better than non-socialised people. They can ask for help from those around them to understand or do something[60]"*.

Imaginations, representations, individual experiences and the culture of risk

To be able to think about far-off aspects, in time or space, of individual issues and practices, it is necessary to take a long-term view, to foresee and anticipate the harmful uses of our personal data and, therefore, to meet the expectations of prevention. However, it is particularly difficult to see the importance of protecting oneself against risks that remain largely intangible.

Beliefs, symbolic representations or cultural structures, which vary according to national context and social group, have an impact on the ability of individuals to attribute meaning to and appropriate prevention discourse. Many meanings are associated with privacy depending on the individual and the social context in which they exist. We do not all have the same ideas or the same representations about what privacy is, and we do not have the same answers when it comes to preserving it. Broadly speaking, we can identify two major opposing views of data protection by individuals: "I have nothing to hide" and "It scares me".

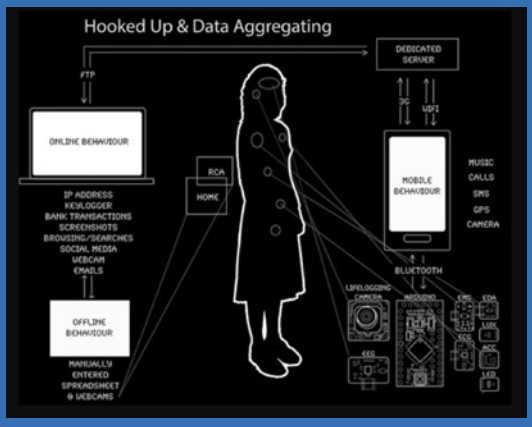
"I have nothing to hide". This discourse is often heard from individuals who are not very concerned about the protection of their personal data. Although it shows that people are aware of surveillance practices, this does not seem to concern them, mainly because of a lack of knowledge or the absence of tangible risks. This discourse is reinforced by the 'inevitabilism'[51] viewpoint promoted by Silicon Valley players and anchored in our collective representations, according to which certain disadvantages of progress are inevitable. "If you want to access a free service, it is inevitable that your personal data will be traded." By not presenting alternatives, this discourse restricts the possible policies: technological choices are not negotiated because they are presented to us as inevitable. It also permeates our collective representations, to the extent that the statement "If it's free, you're the product" is embedded in the behaviour of some individuals, who feel that it is only fair that their data is collected in exchange for a free or better service. On the other hand, the complexity of the digital environment arouses a certain amount of apprehension. The feeling of lacking the technical skills to master it fuels a real mistrust of the tools. Among digitally disadvantaged people, the issue of privacy and the relationship with personal data is a central justification for their non-practice, as Benjamin Bitane, head of training at Emmaüs Connect, points out: *"There is a great deal of apprehension and fear because it's an environment they're not familiar with. We often hear people say: "if I use digital technology, they will know where I live, they will know my card details, etc." They feel that people will break into their homes if they use the Internet'"*[62]. Senior citizens in particular are very apprehensive about digital technology, especially because they are afraid of doing the wrong thing, disclosing personal information or being scammed. They are therefore in a strategy of avoidance, especially when it comes to money or administrative procedures. Benjamin Bitane continues: *"They can use the Internet frequently, but as soon as they have to make an online purchase or pay their taxes, they go to social workers or digital mediators. 'I use the services of a professional, not because I don't have the ability, but because I'm scared'"*. Some people refuse to do certain things online for fear of inadvertent disclosure of personal information.

Furthermore, individual experiences influence the individual perception of data protection and the norm of foresight. In a survey of data breach victims, Dominique Boullier and Maxime Crépel emphasise that this experience has led these individuals to significantly modify their practices[63]. Prior to the breach, they had little or no awareness of the risk. Moreover, they do not know when this violation occurred or why. This uncertainty leads to a feeling of anxiety. Their first reaction is often to blame themselves for the fault. Most of them are then more vigilant and change their practices: stronger passwords, webcam cover, internet cache clearing, ad blockers, etc. Stéphane Koukoui, digital mediator, corroborates this point: *"Once you have had a bad experience, you*

58 Irène Bastard, "Quand un réseau confirme une place sociale. L'usage de Facebook par des adolescents de milieu populaire", *Réseaux*, 2018/2-3 (no. 208-209), p. 121-145.
59 In an interview with LINC, 1 October 2020
60 In an interview with LINC, 4 March 2020
61 Shoshana Zuboff, *L'Âge du capitalisme de surveillance*, Editions Zulma, 2020

are more vigilant. You have to make one or more mistakes before you pay attention[64] *"*. Having been a victim makes one more aware of the risk of having one's personal data hacked and more sensitive to prevention messages.

FRAGMENT OF IMAGINATION



"The artist Jennifer Lynn Morone 'has reached the next inevitable stage of development of capitalism by becoming a business. This model allows you to take advantage of your health, your genome, your personality, your abilities, experiences, potential, vices and virtues'. In other words, the root of the digitisation of the world (in its present form) would be its commodification."

See the off-print: https://linc.cnil.fr/vp2030

***

Data protection benefits from being considered from the point of view of its audiences, supporters and the resistance or the indifference that these prevention messages generate. We need to look at it from the more transverse point of view of inequality and social hierarchies. Not everyone is affected in the same way, has access to the same information or has the same resources or capacity to deal with the consequences. From this perspective, it is advisable to pay attention and give a different message to certain people, certain social groups, according to their particular vulnerabilities.

62 In an interview with LINC, 12 March 2020
63 Dominique Boullier and Maxime Crépel, "Insurance for building Trust and Enabling Big Data", Joint Research Initiative – Axa Research Fund, 2015/2017
64 In an interview with LINC, 13 October 2020

Focus on...

Digitalisation of public services, exclusion and the requirement for self-exposure

The digitalisation of public services, while being a vector of administrative simplification and accessibility that many users are in favour of, at the same time produces new forms of exclusion and makes access to rights more complex for the most vulnerable and least digitally competent people. Citizens must now use digital tools, which they do not always master, to access their social rights, employment or any type of service.

As Benoît Vallauri, head of Ti Lab Bretagne, reminds us, "*The more economically unstable you are, the more you are confronted with dematerialisation*"[65]. While the better-off have little need to use them, for example to pay their taxes, the less well-off often have to deal with digital services. Jobseekers have to update their information every month, others have to submit online applications for the earned income supplement, universal health care cover, training, etc. Faced with the machine and interfaces that they are not always familiar with, the most disadvantaged people are confronted with the need to reveal themselves, and for some, they are increasingly forced to get support, not only socially, but also digitally.

With regard to data protection, some people may be unaware of or have no interest in the subject. "*The subject of personal data is never an issue, people want to access their social rights, they don't care who has access to their data,*" says Benjamin Bitane from Emmaüs Connect[66]. However, Benoît Vallauri[67] points to a difference in trust between the data to be shared for administrative purposes and data shared on social networks on a daily basis, with a greater distrust of the administration than of the platforms. Indeed, as Héléna Revil[68] explains, the problem is not so much the information transmitted as the identity assignment it implies. "*When you give out your personal information, you out yourself into a kind of mould, into an administrative category, and you become defined by your data.*" A person may then feel that they are taking on the stigma associated with certain social identities, "*what people say about people on earned income supplement*", or the "*materialisation of disability*".

Benoît Vallauri notes that people's perception of the digitisation of forms produces "*the feeling among people and social action professionals that the introduction of devices is used for control purposes and to combat social fraud rather than to optimise applications for rights, the feeling that it will be used for control purposes, but rarely in favour of the users*". This is all the more true for social workers who feel that they have become technical advisers on legal aid. Meanwhile, digital mediators must transform themselves into social advisers: "*digital mediation has become confused with social work*", with the feeling for social workers that digital technology "*stands in the way of them helping to empower people*". These social workers can then pass on their distrust to the people they are supporting.

From a data protection perspective, and for less digitally savvy populations, the issue may seem quite remote. Sometimes people don't even have an email address when they go to the counter. And it is not uncommon for the mediators who deal with them to keep their passwords in a notebook so that they can log in again when they come back. These practices have been identified and have already led to the creation of Aidants Connect[69], at the incubator of the Agence Nationale de la Cohésion des Territoires, which provides tools and resources to those who "*regularly support people who struggle with digital technology to carry out online procedures*". In addition, the CNIL regularly recommends in its opinions that alternatives to digital technology be put in place for access to rights or public services, whenever this is associated with the collection of data.

65 Laura Fernandez Rodriguez, Inclusion numérique : "Plus vous êtes précaire, plus vous êtes confronté à la dématérialisation", *La Gazette des communes*, January 2021, https://www.lagazettedescommunes.com/716172/inclusion-numerique-plus-vous-etes-precaire-plus-vous-etes-confronte-a-la-dematerialisation/

66 In an interview with LINC, 12 March 2020

67 In an interview with LINC, 2 July 2020

68 In an interview with LINC, 24 November 2020.

69 https://aidantsconnect.beta.gouv.fr/

Problematic situations that required CNIL assistance

"I cannot live peacefully carrying my entire past behind me."

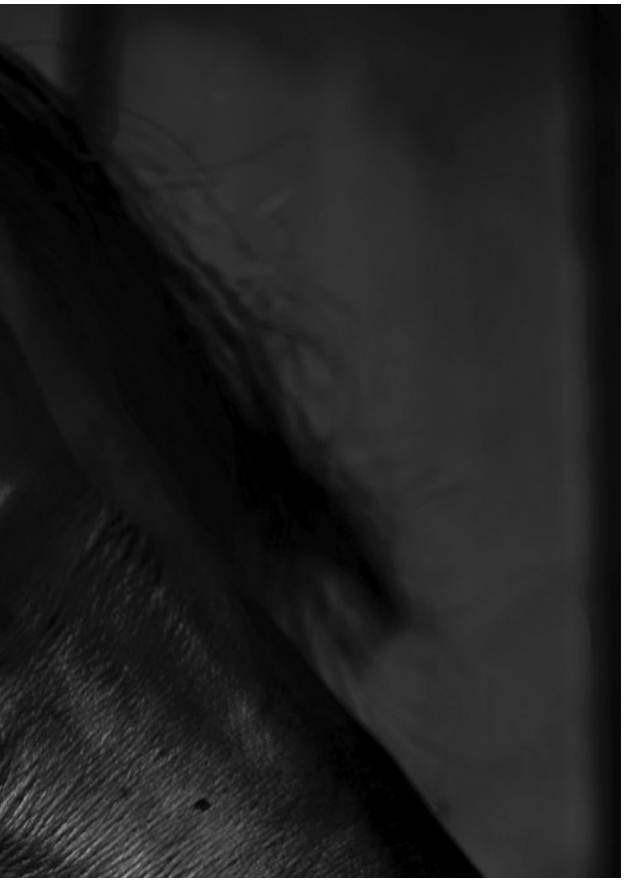
Quentin Lafay, L'intrusion

Problematic situations that required CNIL assistance

While proponents of the *privacy paradox* question why individuals disclose and give access to their personal information, one can conversely ask why individuals rally (or not) for their rights relating to protection of their personal data.

To provide some answers to this question, the CNIL's Digital Innovation Laboratory (LINC) qualitatively studied the letters and complaints received by the CNIL during the months of May 2016 and May 2019[70]. The letters collected and selected contain micro-narratives in which the complainant expresses his or her sensitivity and relates, in varying degrees of detail, his or her experience, the steps taken, the initial investigation he or she undertook, etc. These documents provide information on the situation in which he or she experienced a violation of his or her rights[71]. They also reflect the relationship with the data collection and processing system, the attachments in everyday life to a technical system. Above all, they show the difficulties that individuals face in enforcing their personal data protection rights.
"The requests we deal with are not linked to the social characteristics of the people, but to the situations they encounter"[72]. This remark by a CNIL department head

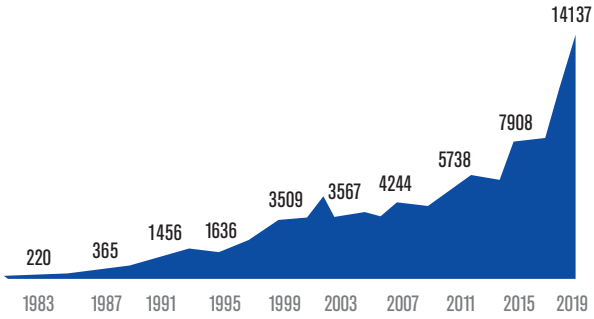
70 The choice of these two dates was intended to explore a possible difference related to the entry into force of the GDPR.
In May 2016, 689 complaints were received by the CNIL (8.9% of annual complaints), 726 in May 2019 (5.1% of annual complaints).
71 The process of enforcing GDPR rights requires the individual to first approach the organisation concerned and then, if unsuccessful, to contact the CNIL.
The scope of this analysis is indeed limited to situations where individuals have not been able to enforce their rights directly with the data controller. Moreover, some of the situations described in the letters and complaints fall outside the scope of the CNIL and are therefore not admissible by the institution.



Pexels - cc-by Kat Jayne

echoes the work of the philosopher Helen Nissenbaum, for whom privacy is always rooted in context[73]. She reminds us that privacy should not be incompatible with the sharing of information, but with the inappropriate communication of information which then violates what she calls "contextual integrity". Contextual integrity differs according to the informational norms, purposes, values and interests specific to each context (technological or social). For example, the same information will be easily shared in a medical context, but its dissemination will be considered abnormal in a professional situation. These informational norms are not restricted to what it is legally possible to collect and disseminate. They include political values, the purposes of the situation, the interests of those involved, the nature of their relationship, the constraints that are imposed, etc. The outlines of privacy thus vary socially and culturally. The complaints and reports received by the CNIL offer an insight into what individuals see as breaches of "contextual integrity", i.e. their perception of technologies and information collection and dissemination practices as a threat to their privacy.

Number of complaints received by the CNIL



Initial consultations of the letters and complaints received by the CNIL are surprisingly varied in terms of the situations encountered and the requests made to the institution. The second initial surprise at the beginning of this research was the low number of calls, letters or complaints that target the big players in the digital economy. Similarly, media cases and scandals have only limited repercussions in terms of complaints received by the CNIL: although expectations of the CNIL are largely focused on these subjects in the context of public debate, and although the institution also has a mission of vigilance and control, it is worth noting that the processing of complaints is part of a very distinct dynamic. Moreover, data protection is not always at the centre of the problem for which individuals approach the CNIL: it is part of a wider problematic situation for individuals (commercial harassment, identity theft, credit refusal, professional conflict, etc.).

Four main situations lead individuals to take action with the CNIL for their rights: when their reputation is threatened by information available online, when they are victims of intrusion into their private sphere through marketing, in the event of surveillance in their workplace, and finally when their names are placed on national registers (banking incidents, criminal records). These four social situations reflect four ways of conceiving privacy and data protection.

72 Head of the Indirect Right of Access Department, CNIL, 3 February 2020
73 Helen Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life*, Stanford University Press, 2010

REPUTATION: REMOVAL OF ONLINE INFORMATION AND DELISTING

In 2016 and 2019, almost a third of the complaints received by the CNIL concerned the unwanted publication of personal data on the Internet: search engines, social networks, online press, etc. The aim of these complaints is to get content available via a search engine delisted or content published in press articles deleted (removal of the article, anonymisation, de-indexing), on social networks or personal sites. They show that people are concerned about their digital identity and want to protect their reputation. These situations are part of a liberal conception of data protection: the right of an individual to control the flow of information about him or her.

Please stop showing my details in search engines. It's unacceptable!! I don't think it's right that my details should appear on the Internet in this way.

(Handwritten letter, May 2016)

These complaints primarily concern the desire to delete information published without their knowledge on websites or social networks, by relatives or strangers. Several situations fall into this category where the type of information published varies: home address or phone number available in online directories, intimate photos published on social networks, comments posted by clients, patients or relatives, removal of the photograph of one's home on Google Street View, acts of defamation contained in blogs, etc.

This URL concerns a part of my former life. I had already asked for this article to be permanently deleted as it may harm me in my new professional life. Please remove this article quickly and permanently. I was tried and sentenced, I have started a new life 200 miles away.

(Complaint, May 2016)

The publication of this information on the Internet is harmful to my reputation and to my social and professional reintegration (search for housing, employment, etc.). Indeed, anyone can access my past convictions, even though I was tried and have paid my debt to society. Today, my goal is to reintegrate into society, to live a normal life, and this type of article does not help me in any way.

(Letter, May 2019)

The second reason for requests is related to the removal of old or erroneous content associated with the identity of individuals, which damages their reputation. These demands are often related to old or subsequently overturned court decisions, such as a person who was investigated but then had the case dismissed. Individuals must first contact the search engines and then apply to the CNIL if they are not satisfied. In France, Google reports that it received nearly 225,000 requests to remove search results since the right to delisting came into force in May 2014[74].

These requests for deletion of information or delisting are indicative of the privacy issues associated with the characteristics of networked public spaces, which complicate the ways in which privacy can be protected, making individuals more vulnerable to 'context collapse', as we describe it in Part 2 (page 16). The indexing by search engines of the traces left by (or on) individuals and their association with their civil identity are shifting the public/private boundaries. In the "contextual integrity" analysis grid described above, the publication of personal information online, i.e. available for any use by anyone, appears to be the most extreme form of "decontextualisation", carrying the greatest risks for individuals. For example, this individual, who has become a prison warden, wants to have his information deleted in order to compartmentalise these different social spheres and thus protect his family.

I would like to ask you to close the pages where my name appears without delay, for security reasons. Indeed, I have just started a new job as a prison guard, and I need to protect myself with regard to the internet and search engines, both for myself and for the well-being of my family.

(Letter, May 2016)

74 Google, Transparency Report, *Requests to delist content under European privacy law*, https://transparencyreport.google.com/eu-privacy/overview

SPECULATIVE FUTURE

Reputable or repudiated

In 2032, reputation is a key metric for everyday life. The ubiquitous and continuous rating has turned this formerly intangible and diffuse social factor into an asset that is measurable and traceable in space and time. As the cumulative sum of traces, reputation is no longer subjective but *data-driven*.

To try to outsmart this rating system and take control of one's reputation, it has become common practice to use digital devices. These tools, "entracers", allow the dissemination of false traces of attendance at events to simulate participation in a conference or trade show.

See the off-print: https://linc.cnil.fr/vp2030

These requests reflect the sensitivity of individuals to privacy and self-exposure. While they do not necessarily have the skills to construct their digital identities, through their searches on search engines, they want to ensure that information about them does not damage their reputation. As such, they seek to define their online self-representation and control the boundaries between their different social spheres. These practices underline that individuals are not passive with regard to their privacy. On the contrary, they engage in reflexive practices to define and manage their personal and social identities by controlling what is visible or not (page 16). This seems to be particularly necessary at a time when reputational capital is becoming a major issue in contexts of greater competition in professional or matrimonial markets[75], where social status is being undermined. Complainants very often mention the importance of their online identity to their reputation (or conversely that the invasion of their privacy is damaging their reputation).

INTRUSION INTO THE PRIVATE SPHERE: UNWANTED MARKETING

The second reason for complaints concerns marketing or political canvassing, which accounts for 15% of the complaints received by the CNIL in 2019 (33% in 2016). In these complaints, in contrast to the previous situation, the breach of privacy is not damage to the individual's reputation, but an intrusion into the private sphere. These situations are an extension of the historical definition of privacy and its protective framework. Contextual integrity is no longer respected as the separation between private space and public and commercial space is blurred.

While not all complainants specify the consequences of these unsolicited letters, calls or emails, some describe the harm suffered. For many of them, the situation borders on harassment and leads to psychological harm.

75 Particularly among the working classes, as Benoît Coquard demonstrates, emphasising the importance of reputational capital and the constant concern to have a 'good reputation'.
Benoît Coquard, *Ceux qui restent. Faire sa vie dans les campagnes en déclin*, La Découverte, 2019

My Mum is elderly, disabled and suffers from a variety of illnesses. She is constantly being harassed on her landline and her mobile. They never stop ringing. (...) It has become too much for Mum to bear, I find her exhausted and crying every night!!! It has to stop, it is having a direct impact on her health.

(Typed letter, May 2016)

Telephone canvassing, which we regularly experience from mostly unidentified individuals. It is a violation of privacy and (...) I'M SICK OF IT.

(Handwritten letter, May 2016)

10 emails a day, impossible to unsubscribe despite web links, phone call to unsubscribe. This harassment has been going on for over a year. It's a shame that these people can ruin lives with impunity.

(Complaint, May 2016)

These situations of unwanted marketing illustrate the insertion of personal data into vast and barely visible technical infrastructures, distributed between several organisations, and over which individuals have little control. The collection of personal data is an issue when this infrastructure invites itself into people's daily lives.

This company approached me by email even though I never gave them my email address. I therefore asked them who or which organisation had given them this information but they were unable to answer. I would really like to know the source of this "leak" because I created this email address expressly for personal use and I never use it on commercial sites. Precisely so I wouldn't get harassed!

(Complaint, May 2016)

I subscribe to [Operator 1] and I receive calls from [Operator 2] to get me to switch over to them. I asked them not to call me again. How did they get my details anyway? Once they even woke me up on my day off. I've had enough. I invoke the Data Protection Act each time, but nothing happens. They always call back. Including again this morning. Nobody is able to remove me from their database. I'm fed up

(Complaint, May 2019)

I ordered products from this site until my dog passed away. On two occasions, when I received advertising emails, I asked to unsubscribe via the link at the bottom of the page. But without success. Yesterday I received another email, and the unsubscribe link didn't work. Today, it's happening again and I tried to send them an email directly through the contact form on their website. But in order to send them an email, I not only have to accept the terms and conditions, but I also have to agree to receive advertising messages! I don't know what to do any more!

(Complaint, May 2016)

Faced with these situations, individuals refer matters to the CNIL when these calls are harmful to them and they are unable to stop them[76]. They thus express a feeling of lack of control, or even panic, when faced with the impossibility of removing themselves from these listings. The case of spam illustrates the difficulties of exercising one's rights in the face of a complex infrastructure, in which the data chain is long. It is difficult for isolated individuals to understand how the opaque market of their personal data used for marketing works, just as the companies that use this information often have no control over this infrastructure.

76 Such commercial solicitations may also be sanctioned by the fraud control authorities for aggressive canvassing. Many complaints thus "escape" the CNIL and are lodged with the fraud control authorities or the energy ombudsman. See for example:
https://www.lemonde.fr/economie/article/2020/09/15/energie-enquete-sur-le-demarchage-telephonique-mensonger_6052194_3234.html

Focus on...

Scams: intrusion into the private sphere and attention seeking

As Finn Brunton analyses in tracing the history of spam, these undesirable activities, which take many forms and fit into the cracks in the networks, have in common that they seek to capture the attention of individuals "*as loot to be seized*"[77]. This intrusion into the private sphere of the individual to seek his or her attention pursues various purposes, more or less legitimate depending on the sender, the medium or the nature of the message: commercial, political or criminal.

This desire to capture the individual's attention leads us to include in this category of complaints the grievances received denouncing online scams, even if they fall outside the scope of the CNIL. Some of them operate on the principle of intruding into people's private lives (by sending emails or letters), in order to capture their attention and phish them by taking advantage of their gullibility. Several types of spam scams can be identified[78].

In this respect, webcam scams are an example of this combination of intrusion and attention: the scammers play on the individual's feelings of shame and guilt and threaten to damage his or her reputation by revealing compromising information that they say they have captured via the computer's built-in camera.

To protect themselves from spam, people must equip themselves with technical anti-spam devices[79] and develop individual skills: recognising fraudulent addresses by knowing how to read an email header, identifying misleading messages, etc. However, less experienced Internet users, who use these technologies mainly for practical purposes (paying their taxes, communicating with their families from a distance, booking train tickets, accessing their accounts, carrying out their professional activity, etc.) are less familiar with these tools and are less vigilant in the face of the techniques used by fraudsters to capture their attention.

As Nicolas Auray describes, fraudsters use techniques to arouse the emotions of the receiver: appeals to shared values (generosity, concern), exceptional promises (financial gain, romantic relationships, better health, etc.), threats (revelations of compromising information, orders for payment, legal proceedings), all the while adorning themselves with the attributes of seriousness (playing on the appearance and similarity with official sites) and fitting into familiar practices to deceive the victim's capacity for discernment. These novices are prime targets for these criminals who intend to take advantage of their gullibility.

In this respect, the calls received by the CNIL during the Covid-19 crisis testify to the distress of part of the population faced with these digital technologies that they are unfamiliar with.[80]

77 Finn Brunton, "Une histoire du spam. Le revers de la communauté en ligne", *Réseaux*, vol. 197-198, no. 3-4, 2016, pp. 33-67. https://www.cairn.info/revue-reseaux-2016-3-page-33.htm

78 Nicolas Auray identifies three: commercial spam (aimed at getting people to purchase products), lottery scams (offering a large sum of money in exchange for an initial payment), and romance scams (love and emotional blackmail scams). Nicolas Auray, "Manipulation à distance et fascination curieuse. Les pièges liés au spam", *Réseaux*, vol. 171, no. 1, 2012, pp. 103-132. https://www.cairn.info/revue-reseaux-2012-1-page-103.htm

79 Nicolas Auray (op. cit.) analyses the techniques put in place by spammers to thwart these technical devices.

80 https://www.cnil.fr/sites/default/files/atoms/files/rapport_cnil_point-etape_covid-19.pdf

PANOPTICON AND THE OBSTRUCTION OF FREEDOMS: SURVEILLANCE AT WORK

Surveillance is the activity of recording and processing the activities of individuals or groups with the aim of verifying the appropriateness of behaviour to a pre-established social norm. From this perspective, the company is a traditional figure of surveillance alongside market and state surveillance. It is exercised in the context of unbalanced social relations, where the hierarchy intends to exercise latent surveillance, or supervision of activity, to varying degrees, for management purposes. Surveillance techniques have evolved in line with the technologies available and the preferred ways of organising work. Supervisors, foremen and managers control activity by physical presence in the workplace or by analysing yields and qualities. Then, automatic badge systems replaced the human controller. Finally, video surveillance and tracking devices have been added to the arsenal of workplace surveillance. These are the two main reasons for complaints about surveillance at work.

Surveillance of employees accounted for 10.7% of the complaints received by the CNIL in 2019 (14% in 2016). The reasons given for setting up the surveillance devices are mainly security issues. However, the purposes of the system are sometimes diverted from these declared purposes to keep an eye on employee activity[81]. However, in order to be legal, these measures must be proportionate, and in no case should the surveillance be constant or permanent. Video surveillance is the most complained about area, especially when the cameras are filming workstations or break areas or can be viewed remotely. Employees complain about the lack of information prior to installation of the cameras, the orientation of the cameras on their activities and their use for management purposes by their employers.

I was told [that the cameras] were only for security and not to spy on us, give us orders or make disparaging remarks.

(Complaint, May 2016)

A camera has been installed and watches my every move. [...] This affects my moods and my desire to go to work

(Complaint, May 2016)

The manager has installed a video surveillance camera above my workstation that films and records all my moves. I am very uncomfortable with this system, and I can't bring up the subject without my manager snapping at me and saying "This is how it is". Do I have to undergo this permanent surveillance? Since I am the only employee, I can't say anything and I'm backed into a corner.

(Complaint, May 2016)

While surveillance is in fact discontinuous, employees feel that they are constantly being watched. Whether or not surveillance is proven, the mere presence of a camera is enough to affect the individual behaviour of employees. As such, it is a powerful control mechanism that leads individuals to conform to what they believe are the norms and expectations of their employer. Beyond the widespread feeling of surveillance, many complaints testify to the use of these devices to control and reprimand employee behaviour.

I am writing to you about several actions my employer has taken against me. I received a text message warning me that I was speeding. I was checked outside my working hours. [while interviewing at another company] I can never turn off the tracking on my vehicle.

(Complaint, May 2016)

My employer recently installed a CCTV system (4 cameras) in our business, several of which film us directly and continuously. This system means that our employer can observe us in real time from home or from his smartphone, and he can call us to give us orders remotely based on what he has observed.

(Complaint, May 2016)

81 https://www.cnil.fr/fr/la-videosurveillance-videoprotection-au-travail

The number of complaints about surveillance in the workplace is related to the availability of these technical devices. CCTV and vehicle tracking devices are now available at affordable costs, making it easier for smaller companies to use them. This surveillance is also part of the evolution of management methods at work.

Hierarchical relations have been transformed to favour a vision of subordination as 'integration into an organisation' rather than 'submission to the orders of a leader'. Rather than direct authority, employees are encouraged to show autonomy in the organisation of work. *"A new form of subordination is emerging: that of allegiance. The bond of allegiance makes one person subservient to the goals of another, who both controls them and grants them a certain autonomy and protection. This new paradigm takes into account both new forms of individual labour relations (salaried or non-salaried) and new forms of company organisation (in production lines and networks)"*[82].

While the control of this autonomy by managers is not unfounded, it must be proportionate and fair, especially when it is exercised with the help of technological tools that process data (images, movements) that go beyond the recording of strictly professional activity. However, the lack of information and transparency of the monitoring systems is rather indicative of a relationship of mistrust in the professional context.

This lack of trust in employees is heightened when work is done remotely, which is highlighted in particular by the use of new surveillance devices put in place by employers during the pandemic crisis (keyloggers, etc.).[83]

In the professional setting that constitutes the source of people's livelihoods, surveillance, which is tending more and more to cover the non-work, private and even intimate sphere, is no longer a simple check that tasks are being performed but acts as a mechanism for controlling individuals as people.

INSTITUTIONAL CONTROL AND BUREAUCRATIC EXCESSES: ELECTRONIC BLACKLISTING

The fourth main category of situations that lead individuals to seek the CNIL's assistance in exercising their rights concerns electronic blacklisting in which names are placed on a register. These cases reflect situations in which individuals are not aware that their names appear on a register and discover (or suspect) it by chance. The Banque de France's registers are the subject of numerous calls, letters and complaints (more than 400 complaints in 2019, more than 500 in 2018), in particular the personal credit repayment incident file (FICP) and the central cheque register (FCC).

The complaints relate more specifically to challenges regarding the appearance on the register of names of people who have since regularised their situation. In the majority of cases, these are procedural failures within credit institutions (revealing the human dimension of the data chain). However, these restrict the ability of individuals to take out new credit.

> *The current blacklisting is therefore both abusive and illegal.*
> *The debt no longer exists, and I only ended up in this situation following a painful and difficult divorce.*
> *I have now found a steady job, on a permanent contract despite being 59 years old. But the fact that I'm on the FICP register is causing me a lot of problems and preventing me from moving forward and rebuilding my life.*
>
> **(Letter, May 2016)**

> *My life is severely affected by this.*
> *I was turned away by the first financial adviser who deigned to see me.*
> *There is a lot of psychological pressure on me because I can't make any plans in the current situation.*
>
> **(Handwritten letter, May 2016)**

82 Alain Supiot, *Le droit du travail*. Presses Universitaires de France, 2016
83 In November 2020, the CNIL published an FAQ on the rights of employees working from home, https://www.cnil.fr/fr/les-questions-reponses-de-la-cnil-sur-le-teletravail

The complainants testify to the difficulties in having their status as victims recognised by banks and financial institutions (although they were previously considered to have had payment problems). In this case, reporting to the CNIL appears to be a means of 1) getting one's status as a victim recognised and 2) putting pressure on the bank. For this, their justifications are both factual and moral. They relate the facts, mentioning the background to their financial problems and how their situation has been sorted out. Above all, they all add to this factual presentation moral values to express their indignation at the fact that they appear on these registers, as a CNIL telephone adviser points out: *"Many of them also feel the need to tell us that they are very honest. That they are in good faith, that they are not bad payers, etc. There is also a moral issue of a situation that they feel is unfair to their personal values".*

Unfortunately, I was put on the register because I exceeded the authorised overdraft by a few euros. My name was added to the register without my knowledge. I am currently in the process of seeking financing for a professional project, which is how I found out about this unfortunate situation. It's a serious problem for me given the urgency of my situation. In fact, it was one of the potential investors who told me my name appeared on the register. So I quickly remedied this problem, unlike the Bank which is dragging the situation out causing me enormous damage.

(Complaint, May 2016)

I accidentally wrote a cheque for €300 on a closed account. I did not realise and received notification that I was being put on the register.

(Complaint, May 2019)

I was recently refused a credit application by my bank and was surprised to learn that my name was on the FICP register. I contacted the Banque de France to find out who the establishment was. It was [a credit institution], although I paid off the revolving credit in 2016. Despite a first letter sent in September 2016 and a second one in June 2018, the company did not see fit to reply to me.

(Complaint, May 2019)

These situations relating to blacklisting echo the collective mobilisation and debates of the 1970s that led to the French Data Protection Act. Faced with the computerisation of State services and citizens' files, tensions are arising over the data collected, how it is used, the length of time it is kept, the interconnection of files and the possibility for individuals to intervene in this data. At the time, there was collective mobilisation against these plans to establish electronic registers. Here, the denunciation is individual and is aimed less at the legitimacy of these registers than at the lack of updating.

Focus on...

Historical grounds for complaint

Marketing, reputation, surveillance at work and electronic blacklisting have been recurrent grounds for complaints since the creation of the CNIL. The institution's annual reports give an overview of the constancy of these problematic situations, despite the progressive changes in their form and the emergence of new technologies and uses.

Since the creation of the CNIL, **marketing** has been one of the main reasons for complaints. It was the first concern highlighted in the first annual report: "*On several occasions, the Commission has received complaints from individuals complaining of being annoyed by advertising that has reached them at home without their consent, and sometimes, and this is obviously more serious, at their workplace.*" These advertising mailings will evolve with the development of technology: telephone calls, faxes, SMS and emails will be added to postal mailings. Spam – a term whose origin, a Monty Python sketch, is discussed by the CNIL in its 22nd annual report – led the regulator to experiment in 2002 with an email box allowing individuals to send their requests by email, and the CNIL to study the content and senders[84]. This mission is now performed by the association Signal Spam[85].

The question of what an individual can do **in the face of electronic blacklisting**, particularly administrative blacklisting, which is at the very origin of the institution, is a key issue in the CNIL's actions and is one of the recurring reasons for complaints. Apart from marketing, banking, taxation and credit are regularly among the main reasons for complaints from individuals. In 1985, for example, "*complaints about names appearing on a register of bad payers leading to the refusal of credit*"[86] were among the main causes of solicitations by individuals.

Surveillance at work is a topic that quickly led the institution to intensify its work, starting in 1983: "*the impact of information technology on labour relations and the dangers that uncontrolled development of this technology could pose for freedom of work led the Commission to set up a sub-committee responsible for this sector*". In its 1987 report, the CNIL noted that a "system" in which "people working under the surveillance of a camera" was "destined to undergo a certain development"[87], and from 2000 onwards, the emergence of "internet monitoring of employees" was noted.

Finally, the **reputational issue**, linked in particular to the question of advertising information in newspapers (see part 1 on page 30), is becoming increasingly important with the advent of the Internet and the retention of online data after they have been indexed by a search engine. In 1997, the CNIL mentioned, by way of illustration, the risk of information stored in "newsgroups"[88], which could be easily retrieved via a search engine – and even more so in 2012 when the system of "tagging" photographs, adding the image to the information, became popular. The right to delisting, by making the rights to object and erasure of the 1978 French Data Protection Act operational in the particular operating system of search engines, will make this issue of online information control more visible from 2014.

84 "In the space of three months, approximately 325,000 spam messages were received, which demonstrates the mobilisation generated by the "spam box" operation, with Internet users finally finding an institutional relay for the problem of spamming, which they are often powerless to deal with, both technically and legally."

85 https://www.cnil.fr/fr/spam-phishing-arnaques-signaler-pour-agir

86 There are two types of requests from individuals: • complaints about questionnaires to be filled in; • complaints about names appearing on bad payer registers leading to credit refusal.

87 The CNIL decision of 15 December 1987 sets out a certain number of essential guarantees for people working under camera surveillance, a system that is bound to develop further

88 Thanks to these newsgroup search engines, it is possible, from one of the messages you have sent, to retrieve all the other contributions you have made on all the other newsgroups and thus to obtain a fairly clear profile of your interests.

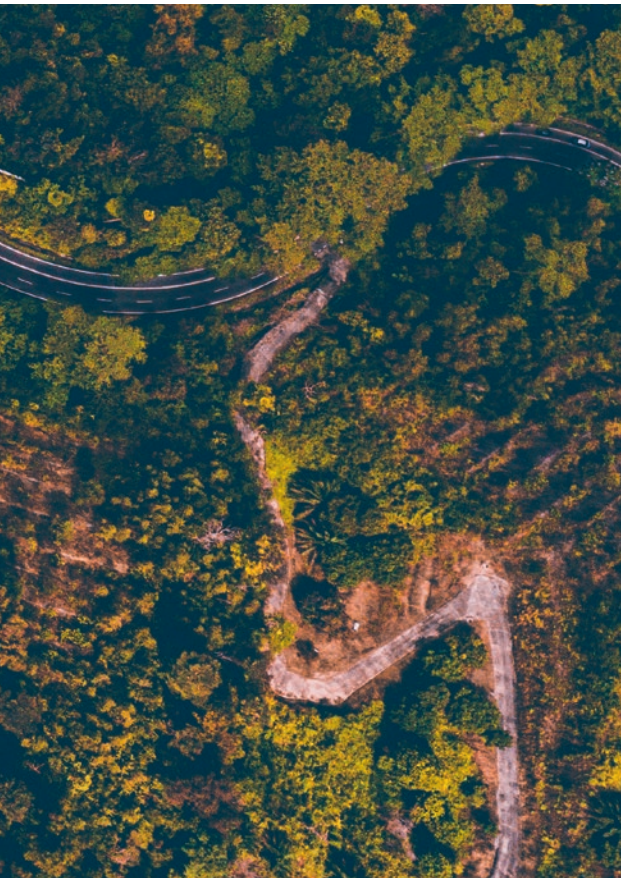
Exercising its rights: the stages prior to contacting the CNIL

"You can't break chains
if you can't see them"

Franz Kafka, The Trial (1933)

Exercising its rights: the stages prior to contacting the CNIL

As well as the diversity of these situations, the complaints show the paths taken by individuals, a journey with many obstacles to navigate before they can assert their rights with the CNIL.
The exercise of rights is the result of an uncertain process, in which the data infrastructure has to be made visible, and the individual has to consider himself a victim of the data processing and be in an unbalanced social situation that prevents him from solving the problem himself.



Pexels - cc-by Deva Darshan

MAKING THE DATA INFRASTRUCTURE VISIBLE

The exercise of rights requires awareness of the collection and processing of personal information. However, these operations are embedded in complex infrastructures that are not very visible or understandable for the individual to understand. A prime example of this complexity is that of online advertising, where, despite the collection of consent through "cookie banners", Internet users have little understanding of the entire data chain and of who has access to it[89]. This requires knowledge of how it works from a technical point of view, the legal framework and the ecosystem of the data market. Above all, manufacturers sometimes tend to make this operation as elusive as possible for the layman. Their aim is to provide the most seamless experience possible through technology, particularly through their work on interface design[90]. This poor visibility of the infrastructure makes it difficult for individuals to realise the extent of the data collection and processing. Who are the operators of the shift towards awareness?

Although high-profile cases play a role in revealing how certain companies operate, they lead to few complaints being filed with the CNIL. *"We do not receive many complaints in reaction to current events, following scandals that may appear in the press. (...) This remains marginal in relation to the total number of complaints. For example, there was no massive influx following the Snowden revelations"*[91]. This limited effect of high-profile cases on the lodging of complaints is partly explained by the fact that these revelations, while they reveal malfunctions and abuses in the collection of personal data, are not accompanied by a victimisation process (see below).

> *When I want to buy tickets online for a visit or a show, I have to give my surname, first name, date of birth, email address, postal address, telephone number, etc. When I buy a ticket at the box office, I am not asked for any of this information. For a simple ticket online, is the request for our full contact details justified? Shouldn't the protection of personal data apply to these establishments?*
>
> **(Typed email, May 2019).**

The critical awakening to data collection takes place during particular operations, where the attention of individuals is heightened, such as registering for a service or making an online payment, which are moments of distension between the streamlined experience of the calculated company[92] and the sensitive world of the user. It is also particularly present when searching on search engines which facilitate the visibility of information available online.

89 See the LINC articles that highlight this complexity and explain how these online advertising players operate. https://linc.cnil.fr/dossier-cookies
90 See IP report No. 6 *Shaping Choices in the Digital World*, 2019. https://www.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf
91 Interview with complaints department managers, 15/01/20
92 The term "calculated company" refers to a digitised company whose functioning is subject to algorithmic calculations.

Focus on...

Complaints, a step in the CNIL's control process

The CNIL has in place a complete control process enabling it to receive alerts through various channels, including complaints, and then to carry out controls. The consequences can range from closure or order to financial or other sanctions. In some cases, publicity may be decided upon depending on the seriousness of the case.

Data infrastructure malfunctions are the source of many complaints: when there is an error, a breakdown, a data hack, a glitch in the algorithm, a maintenance fault, unsolicited emails, identity theft, etc.[93] The breakdown, far from being a simple technical failure, reveals the socio-technical network, which is invisible in day-to-day operation. The origin of the failure may be technical, human or organisational, intentional or unintentional.

"Removal from the register impossible due to a computer problem related to married name/maiden name. Apparently, the account was created with the wrong name. I can't be removed from the register because the names don't match."

(Complaint, May 2016)

"I received an online receipt for purchases from [a retailer] to my email address, even though I do not have an account with [this retailer] and have never shopped at [this retailer]. After checking, it seems that someone has created an account linked to my email address, but I can't log in because it's not me, and I refuse to have my email address linked to fraudulent transactions like this."

(Complaint, May 2019).

"Yesterday, we logged into our [credit institution] customer area to request early repayment statements for our zero interest loan for June, July and August 2019. We submitted several requests and, for one of them, we were surprised to receive a repayment statement for Mr XXX, a gentleman who is totally unknown to us. For another request, we got a mixture of our information and this gentleman's information. Following this dissemination of personal data, we are quite understandably concerned about the protection of our own personal data. How can [this credit institution] guarantee us that our data is protected after it sent us the data of a third party?"

(Complaint, May 2019)

By disrupting the routine functioning of data infrastructures, frictions and malfunctions make them visible to individuals[94]. Failure of these infrastructures is the source of many of the problems posed by data collection for individuals. It is a necessary, but not sufficient, step to accessing rights. Individuals must also make a moral judgement about this data infrastructure and see themselves as victims of the situation in order to seek compensation.

FRAGMENT OF IMAGINATION

"A huge public screen with an error message on it makes you imagine what it would be like if its function was to intentionally publicise data leaks or other misuses."

See the off-print: https://linc.cnil.fr/vp2030

93 Like algorithmic 'glitches' that reveal the routine operation of algorithms.
Axel Meunier, Donato Ricci, Dominique Cardon and Maxime Crépel, "Les *glitchs*, ces moments où les algorithmes tremblent", *Techniques & Culture*, https://journals.openedition.org/tc/12594

94 In this respect, the CNIL has repeatedly recommended the introduction of "desirable frictions" to make data collection and processing visible.
See in particular the IP report *Shaping Choices in the Digital World*, the design.cnil.fr website and the white paper *À votre écoute*.

FEELING VICTIMISED

Every day, people encounter problems that they attribute to the collection or processing of their personal data. Yet only a minority will do anything to change the situation, while the vast majority just put up with it. Indeed, in order for an individual to take action, the damage must become real harm: it is often necessary for the lives of individuals to be *affected* socially, morally, psychologically and/or economically for them to consider themselves victims of the situation.

For example, a couple with healthy bank accounts have three cheques refused in two supermarkets where they usually shop. This unfortunate experience makes them aware of the *scoring* systems put in place in these stores to identify unpaid cheques. This couple feels that they have been harmed in a way that offends their moral values. As well as the actual refusal of the cheque, the social situation in which this malfunction occurs (a supermarket they normally go to) damages their reputation and impacts their social image.

> *We recently went shopping in two shops: 3 cheques were refused by these establishments for no reason. We suffered moral prejudice because we were in a queue at the checkout with people we knew. (...)*
> *In our case it is an attack on our freedoms because their refusal criteria are based on assumptions and not on bank account statements to which they have no access. Knowing that our personal situation is more than comfortable and being refused a cheque in a place where we are known is a harmful and unpleasant situation.*
>
> **(Typed letter, May 2019)**

Another example is that the unwanted dissemination of information online can contribute to the stigmatisation of the individual concerned, giving him or her an identity marker around which his or her social interactions will be reconfigured in a negative way[95]. This can lead to psychological harm to the individual and may offend his or her principles and moral values. Similarly, the refusal of a bank loan due to an erroneous entry in a delinquency register, in addition to the economic damage, is also a social and moral offence experienced as an attack on the honour of individuals. By concluding their complaint with the phrase "You have sorted out your situation and still appear on the register", many of them testify that this situation conflicts with legitimate principles of justice in modern Western societies, such as the right to a second chance. Thus, the complaints reveal a moral sense, inscribed in a grammar of what is fair or unfair, through which individuals interpret the situation experienced.

FRAGMENT OF IMAGINATION

Digital equivalents of street-medics, set up to provide relief, site-medics are volunteers who treat physical and psychological ailments linked to the use of digital technology, which are not recognised by occupational medicine or traditional social security.

See the off-print: https://linc.cnil.fr/vp2030

Becoming a victim also means attributing responsibility for the offence to a third party. However, many people feel responsible for their situation, for example because of their negligence in giving out personal information or their gullibility in the face of scams. In cases of Internet scams, Nicolas Auray notes that feelings of guilt and shame lead victims not to lodge a complaint. They are often afraid of being mocked at the police station[96].

95 E. Goffman, *Stigmate : les usages sociaux des handicaps*, Paris, 1975
96 Nicolas Auray, "Manipulation à distance et fascination curieuse. Les pièges liés au spam", *Réseaux*, vol. 171, no. 1, 2012, pp. 103-132.

"Not many people come to us with problems of identity theft, online harassment or phishing. They feel ashamed, that they have been tricked, that they were too naive, that they gave out too much information when they shouldn't have."[97]

Stéphane Koukoui, digital mediator, Rennes

This sense of guilt is reinforced by the implicit norm that data protection is based on the behaviour and actions of the individual (see Part 1, page 18). The damage suffered is therefore interpreted as a personal responsibility. However, it is generally understood by both digital training (and regulatory) bodies and by individuals themselves as a risk associated with any digital practice, a difficult-to-avoid secondary consequence of our digital environment and economy which forces us to expose and disclose. Individuals are asked to acquire skills, implement good practices, adopt "digital hygiene", be careful in their use of digital technology, etc.

Focus on...

Complexity of the infrastructure, dilution of responsibilities

The case of spam illustrates the difficulties of exercising one's rights in the face of a complex infrastructure, in which the data chain is long. It is difficult for isolated individuals to understand how this market of their personal data used for marketing works, just as the companies that use this information often have no control over this infrastructure. This lack of knowledge may be deliberately maintained by advertisers, but the complexity is often beyond them. Some companies buy lists of prospects from routing companies or other data brokers and/or outsource mass mailings or calls to them. They are then unable to remove complainants from the original database who continue to receive unwanted advertising.

I have asked several times (as far back as 2014), by phone or by email, to be removed from [company XX]'s database. In spite of this, I still receive several emails a day from them. I got [the director of company XX] on the line herself, who told me initially that she would sort out the problem and then basically said that I had to contact the companies from which she buys files myself. Outrageous!

(Complaint, May 2016)

Another testimony, published in Le Monde, is that of an engineer specialising in computer security who has been receiving several calls a day for several months. He decided to trace his registration in the call lists, but came up against the complexity of the data chain. "*It's impossible to know who sold my number: I'm unlisted, I've called all the providers who have my number. They all confirmed that the box on my contract prohibiting the resale of my personal information was checked. When I ask the operators who gave them my number, I am told that it was ERDF [the former name of Enedis] that sold my number, which is impossible!*"[98].

In fact, cold callers use a variety of lists, made up of scattered information gathered here and there: they purchase listings on second-hand markets or files from third-party companies (removal companies, etc.), they collect numbers online using specialised software, etc. In the end, no one in the chain knows the source of the information.

97 In an exchange with LINC, 13 October 2020

98 Damien Leloup, "Démarchage dans l'énergie : un important marché de revente de fichiers clients", *Le Monde*, September 2020, https://www.lemonde.fr/pixels/article/2020/09/15/d-ou-viennent-les-numeros-appeles-par-les-centres-d-appel_6052211_4408996.html

Discourses on the prevention of personal data protection are tantamount to placing the responsibility for their own protection on the individual. They thus legitimise an implicit theory of responsibility that identifies the 'source of trouble'[99] as the behaviour of individuals. The dominant interpretative frameworks generally lead the individual to see the harm he or she has suffered as the result of a mistake on his or her part. In order to make use of one's rights, it is essential to redefine one's experience as a situation of injustice for which responsibility is attributed to someone other than oneself.

Shifting this blame is not self-evident, as it is sometimes difficult for the individual to identify the person responsible for the data collection. As mentioned earlier, data infrastructures are complex and involve many parties, which are hard for the individual to identify. Many parties are involved in the data chain and could, as such, be considered by individuals as having a share of the responsibility[100]. For customers who have had a cheque rejected, should the responsibility lie with the supermarket chain using this service? Or with the company developing the *scoring* system? The attribution of blame leads them to conduct an investigation to demonstrate the link between the data collection and the harm suffered.

Finally, the victimisation process requires awareness of one's rights. The law facilitates awareness of the harm suffered, legitimises victim status and provides support for action. However, knowledge of data protection rules is not evenly shared. Many of the people who contact the CNIL do so to seek advice regarding their rights, particularly through letters or phone calls. They want to rid themselves of the legal uncertainty in which they find themselves (do I have rights in this situation that I consider unfair?) and to find out how to enforce these rights. The laws are complex, and their mastery by individuals is far from assured, especially since it is necessary to align their particular situation with an abstract legal category.

Lawyers or other legal advisers (trade unionists, social workers, civil servants, etc.) traditionally help individuals to translate their grievances into the language of the law and to make general sense of these individual cases. However, few letters or complaints explicitly refer to the register and the legal categories. Allegations are generally more moral than legal. References to the GDPR or to the French Data Protection Act are rare and often not very precise. This work of legal translation of the moral indignation of individuals is carried out by CNIL agents, who acknowledge their status as victims by qualifying the breach that constitutes the harm and have it recognised by the organisations concerned so that the situation can be changed.

Focus on...

The CNIL, an entry point for digital issues

"*The people who contact us are often in a situation they consider problematic. They are aware of this, but they don't know what to do. Sometimes they call us without really knowing whether their issue falls within the CNIL's remit. Indeed, many of them start their call by saying "I don't know if I'm in the right place" or "I'm sorry to bother you". Our role is to give them information on their rights, whether they are related to the CNIL or not. With experience, we are able to advise them and direct them to a particular authority that can solve their problem*[101]." With six legal offices, including a general office open every morning, the CNIL receives many questions outside its field of competence among the 25,000 calls received each year. It acts as a referring institution in the minds of certain individuals for any problems closely or loosely related to the digital world and the Internet. "*In general, people don't really know what the CNIL is for. They contact us for all sorts of problems they encounter related to the Internet or their smartphone: from cyberbullying on social networks and webcam scams, cameras filming the street or the neighbour's house, identity theft, their names being placed on the register by their bank, teachers' video-conferencing courses, or even employer surveillance of people working from home. They also contact us because they don't always know who to contact. We also see that in certain situations the support systems are not complete or even sometimes in their infancy and that users may have up to four contacts from different public departments for an urgent problem, which increases his or her distress, for example in situations of cyberbullying of teenagers*[102]."

99 Joseph Gusfield, *The Culture of Public Problems: Drinking, Driving, and the Symbolic Order*, Economica, 2009, p. 51.
100 Even if they are not considered to be data controllers within the meaning of GDPR.
101 Exchange with a telephone advisor from the public relations department, 6 February 2020
102 Exchange with heads of public relations, 26 May 2020

REVERSING THE BALANCE OF POWER

In addition to the feeling of being a victim and the awareness of one's rights, there is a third condition for recourse to the CNIL. It relates to the distribution of power, resources and constraints specific to the situations in which complainants find themselves. Unable to assert their rights with the organisation concerned, or to extricate themselves from the situation by their own means, individuals turn to the CNIL to shift the balance of power in their favour.

The traditional process for asserting one's data protection rights requires them to contact the relevant bodies directly. Although it is not necessary to consider oneself a victim in order to request activation of one's rights, their activation is often a process of victimisation. Individuals should therefore first try to resolve their problem themselves with the organisation responsible for data collection and processing by making initial contact. In some cases, they may implement avoidance strategies to reduce the influence of the companies in question, such as using ad blockers in browsers or changing some of their practices (e.g. changing social networks or travel routes). If these attempts fail (difficulties, lack of response, unsatisfactory response), they can then seek the support of the CNIL and move beyond the self-interest of the parties concerned. The process is thus long, tumultuous and uncertain for individuals who often find themselves isolated in an unbalanced power relationship, which limits their ability to enforce their rights.

First, they must be able to identify the organisation responsible and obtain its contact details. This is a tedious process when a host of players, forming a network of intermediaries that is difficult for users to understand, are involved in the processing of their data. It is difficult to know how their phone number ended up on a call list, or to determine the publisher of a website from which they want to have information removed.

The complainant does not have all the information necessary to know who is responsible for his or her problem and to make a complaint.

Focus on...

"Promoting competition", a strategy that only works in some cases

When a user is dissatisfied with an organisation's handling of this data, one strategy is to stop using the service in question in favour of a competitor perceived as more protective. This dynamic was illustrated recently when WhatsApp's contractual conditions changed, leading to greater use of third-party solutions such as Signal or Telegram. The GDPR has also embraced this approach with the "right to portability" which is supposed to make it easier to switch providers by "porting" one's data from one service to another. However, this right is not well known and not widely used in practice, and will rarely be a solution if the organisation does not already respond to the exercise of a right to object.

More broadly, the 'competition' argument may work in markets where there is little friction and where products and services are standard and interchangeable between different players, such as trade in goods.

Conversely, when the data processing is linked to a subscription (cable, bank, electricity), changing supplier will be complex, especially for personal data issues only. Similarly, in the case of communication services (messaging, social networking, email, etc.), network effects can make the change difficult. Finally, in many cases, competition does not exist, as in the case of public services or services with a monopoly or quasi-monopoly.

I want to delete all of my sports results that are on this page. The site refuses to delete them without me providing my ID card. Knowing that they are already using my personal data without my consent, I don't trust them and do not wish to disclose such information to strangers by email.

(Complaint, May 2016)

If they are able to identify the organisation responsible, they still need to be able to enforce their rights. Some complaints state that it is impossible to assert one's rights in the absence of mechanisms (contact forms or data modification forms, email address, non-digital procedure) to contact the organisation or when the information was put online several years ago and they no longer have the password to access their account, which can lead to Kafkaesque situations where to delete their account, they must log in, which they can't do because they no longer have their login details.

I'd like to remind you that I'm currently in prison and therefore don't have access to websites, so I can't fill in any online forms. So I would like to have an alternative way of filling in these forms please, handwritten would be ideal.

(Handwritten letter, May 2019)

I would like to delete a very old blog that I had when I was younger. Given how old it is, there is no way I can remember my password from that time. The same goes for the email address that was linked to it. It was an @yahoo.fr email address but I can't find my user nameor password. So I am coming to you to delete this blog, which has not been active for years.

(Complaint, May 2016)

Having cancelled my subscription with [Internet operator] more than 2 years ago, I did not think that my "personal page" service was still open and had content on it. I've contacted [the Internet operator] several times, but as this subscription is cancelled with them, they cannot delete these personal pages.

(Complaint, May 2016)

These complaints illustrate the physical registration necessary for the application of the law. Frictions to the implementation of these rights also materialise in the additional requirements, often for good organisational reasons[103], but not always necessary, requested by companies: providing a copy of one's identity document, sending the request by registered mail, etc.

I would like to remove all my information from the site because I did not request it and it is wrong. It is simply impossible to contact them, I get no answer to my emails or they just bounce back.

(Complaint, May 2016)

I was a customer of [a telephone operator]. After cancelling my contract, I carefully followed the procedure to request in writing that all my personal data held by this operator be deleted. Not only is it still active on their website, but this operator continues to use it for marketing. All they have said in response is that I should submit a new request! Of course, this operator does not provide any way of contacting them and solving the problem...

(Complaint, May 2016)

I am still receiving emails from them even though I unsubscribed a few months ago. What's more, if I click on the unsubscribe link in the emails, it says that I am already unsubscribed. I want them to actually remove me from their mailing list.

(Complaint, May 2016)

103 Such as ensuring the identity of the applicant before transmitting personal information: see Kashmir Hill, *Want your personal data? Hand over more please*, The New York Times, January 2020, https://www.nytimes.com/2020/01/15/technology/data-privacy-law-access.html

I have repeatedly sent requests to stop SMS advertising from [company XXX] ("STOP" by return SMS) and I continue to receive SMS advertising on a very regular basis.

(Complaint, May 2019)

The temporal management of their claim, in the hands of the organisations, is another illustration of the unfavourable balance of power for complainants vis-à-vis these organisations. A number of complainants are in urgent situations that cannot tolerate the lengthy administrative processing of their application. However, response times are often long, in the region of several weeks or months... if they get a response at all. And yet, the GDPR requires data controllers to respond "without undue delay" and within one month, unless the request is complex (Article 12(3) of the GDPR). All these difficulties complicate the process of accessing rights for individuals, who are in a situation of imbalance vis-à-vis these companies, as researcher Paul-Olivier Dehaye points out: *"These obstacles are not to be downplayed. There is such an imbalance between the person requesting the data and the*

Focus on...

Mostly individual complaints, little collective mobilisation

This recourse to the law, contrary to what is observed for other situations such as complaints of discrimination[104], is very rarely associated with a collective (trade unions, associations, lawyers, etc.) acting as an 'operator for legal mediation of the complaint'. The victim intervenes in his or her own name, sometimes assisted by a close relative (parents, children, etc.); complaints lodged by a legal entity who takes charge of the case are few and far between[105].

Within the framework of the CNIL's complaints system, whistleblowing is restricted to the interaction between the complainant and the institution and is not intended to form an "audience"[106]. It is thus essentially an individual action exercised in a private setting and aimed at asserting one's rights and repairing damage, and not a political action that mobilises a collective to defend a cause within a public arena in the name of collective values. Most people's indignation is accompanied by a desire to find a practical solution to the problem rather than to publicly incriminate somebody and cause a scandal. In other words, people who approach the CNIL with complaints are defending *their* privacy rather than *privacy*.

Work to look at the more general picture is carried out after the fact by the CNIL, which aggregates the scattered cases into a collective cause and initiates control procedures, which may go as far as public sanctions.

However, there are exceptions to these individual approaches. The GDPR has indeed introduced the possibility of collective action. Since its entry into force, several associations have lodged collective complaints with the CNIL. For example, the Quadrature du Net filed a complaint on behalf of 12,000 people in May 2018 against Google, Apple, Facebook, Amazon and LinkedIn; the NGO Noyb *(None of Your Business)* on cookies and data transfer in 2019 and 2020; or the Ligue des Droits de l'Homme in June 2020 denouncing the difficulties of exercising drivers' right of access with Uber. These collective complaints have the characteristic of being mediated by these organisations. They are accompanied by press releases, press conferences and media coverage. As much as to change a situation that is detrimental to individuals, this media coverage aims to alert the public, provoke a "scandal" and put these problems on the agenda of public debate.

Furthermore, the CNIL also has the task of acting, on request or on its own initiative, against processing carried out or planned, and often on questionable behaviour exposed in public, outside the specific framework of complaints processing.

104 Vincent-Arnaud Chappe, *L'égalité au travail. Justice et mobilisations contre les discriminations*, Presses des Mines, 2019, 210 p.
105 They do exist, however, such as the recent complaint by the Ligue des droits de l'homme against Uber to allow drivers to access their data. https://www.liberation.fr/france/2020/06/12/la-ligue-des-droits-de-l-homme-depose-plainte-contre-uber-devant-la-cnil_1791034
106 It should be noted that some complainants do, however, publicise their complaint and their exchanges with the CNIL on social networks.

company concerned that the slightest friction will amplify this imbalance. This is far from inconsequential. I place some of the responsibility for these obstacles on companies, although some have legitimate reasons to be cautious. A range of abuses is possible[107]*."* This lack of response leads individuals to lodge a complaint with the CNIL, hoping to get a hold on the organisation concerned. Since they cannot resolve the situation themselves, the support of the CNIL should shift the balance of power in their favour.

Finally, the relational framework of certain unbalanced social situations reduces the possibilities for the individual to voice their rights for fear of repercussions. This last case is common in professional situations: several complainants explicitly mention protecting their anonymity so that their superiors do not know about their whistleblowing: *"could you also keep my identity anonymous to my employer"* (complaint, May 2016), *"I would like to remain anonymous"* (complaint, May 2019). Thus, the individual relationship to the right to personal data protection is embedded in situations where the positions and resources of power in the organisation vary. Other individuals, with a higher hierarchical position, particular resources or the support of a trade union, are inserted in a forcefield that is more favourable to them and means they do not have to resort to the CNIL to assert their rights. Others, on the other hand, do not even think of challenging a situation they consider unfair and undertake in silence.

The complainant perceives the CNIL as a resource, which will enable him or her to objectify his situation, rationalise his or her discourse and use the law to get a grip on a situation that is beyond his or her control and to shift the balance of power in his favour.

> *A little disappointed by the impregnable fortress YouTube that stands before us, we are contacting you to ask for your help to get this famous video removed.*
>
> **(Complaint, May 2016)**

> *Please find enclosed a complaint I sent to the company XXX. Can you help me because I'm not getting anywhere by myself. I have contacted them by email several times but to no avail, so I'm turning to you.*
>
> **(Typed letter, May 2016)**

> *They are refusing to do anything, so I am asking you to put pressure on them to get my name removed from the register as soon as possible.*
>
> **(Typed letter, May 2016)**

A very large number of complaints and letters contain expressions such as *"I don't know what to do any more"*, *"I'm fed up"*, *"I've had enough"*, *"I'm tired"*, etc., which testify to the weariness of individuals, engaged in long and fruitless procedures, and feeling powerless to solve their problem. Faced with these difficulties, it can be assumed that many people do not exercise their rights. Rather than engaging in whistleblowing *(voice)*, they accept or suffer the surveillance in silence *(loyalty)* or turn to other technical environments and infrastructures, or even stop using digital technology *(exit)*[108]. As the sociologist Bénédicte Rey states, *"taking regulatory and legal steps therefore requires the user to invest time and cognitive resources, which represents a significant cost for a result that is not guaranteed"*[109].

This necessary cost leads to inequalities in the exercise of rights between individuals[110]. Not everyone has the time, knowledge or money to devote to protecting their personal data. Depending on the devices for accessing rights implemented by the organisations and the skills of individuals, the routes become longer and more complex for some. Therefore, even though the number of complaints received by the CNIL is increasing every year, there is no doubt that still too few non-compliant data collections and processing are noticed and fought by individuals.

107 Quoted in Le Temps, https://labs.letemps.ch/interactive/2020/longread-donnees-personnelles/

108 According to Albert Hirschman, users have a choice of three behaviours when faced with the failure of a public or private institution: exit, voice or loyalty.
Albert Hirschman, *Défection et prise de parole*, Fayard, 1970

109 Bénédicte Rey, *La vie privée à l'ère du numérique*, Lavoisier, 2012, p. 134

110 The materials at our disposal only provide fragments of descriptions of the social situations of individuals. These initial analyses should be supplemented by a survey of these complainants to obtain more information on resources, constraints and power relations specific to the individuals (their social properties) and the social groups to which they belong.

Beyond individual rights, collective tools for protecting privacy

"New Artificial Intelligence was expected to solve the world's problems.
But to every question, it invariably replied that data was missing."

François Houste, Mikrodystopies

Beyond individual rights, collective tools for protecting privacy

Since 1978, the CNIL's activities have been part of the fundamental right of each individual to the protection of his or her data, private life and freedoms in the face of the development of computerised systems. By being derived from fundamental rights at the heart of modern democracies, data protection incorporates a powerful normative system that is firmly rooted in Western societies. However, these individual rights raise the question of the relationship with the collective and how it would be possible to ensure that they are respected, no longer in a balanced relationship, where the individual, alone against an organisation, seeks the support of an authority with necessarily limited means, but in a more balanced power relationship between social groups. Today, the CNIL ensures that it responds as best it can to the needs of the complainant and, if necessary, initiates measures ranging from controls to sanctions in order to bring into compliance those players who have not respected the framework (see infographic on page 42). It often uses individual situations to carry out an analysis that concerns a large group of people, users or employees of the organisation in question, and the complaints constitute for it a fine sensor of society's expectations. However, it receives

Pexels cc-by Ann H

more than 14,000 complaint applications each year and its resources, while increasing, make it difficult to respond quickly to so many questions and individual requests.

The CNIL's mission is first and foremost to act as the "guardian of rights and freedoms": the regulator is not intended to be merely the "personal data police" or "the GDPR forces". A better understanding of the reasons why people find themselves asserting their rights with the CNIL and more detailed knowledge of the individual and collective reasons why individuals protect their freedoms should enable us to respond to these challenges. It is still the CNIL's policy to ensure that players (data controllers) are brought into compliance, through penalties and sanctions, but also through support and the production of tools that will enable them to better take the GDPR and the various applicable laws into account.

The CNIL is not alone in dealing with individuals on the one hand and data controllers on the other. Individual rights are also a collective matter. Combined with the actions of the CNIL, the creation of new intermediary bodies for data, the consideration of these issues by trade unions, but also the actions of associations, the State and local authorities, and the contributions of research, can help to strengthen the protection of data and privacy. This set of recommendations thus provides some guidance.

CONTINUING THE WORK UNDERTAKEN, BOTH INTERNALLY AND WITH THE RESEARCH COMMUNITY

This Innovation and Foresight report looks back at the history of privacy protection and then, in a comprehensive approach, at ordinary practices in the management of personal data by individuals. It includes an unprecedented exercise in qualitative analysis of complaints received by the CNIL. This in-house study calls for further research, in conjunction with academia, to better understand the digital uses and legal routes taken by individuals. This knowledge is necessary for the institution to support individuals in protecting their data and freedoms.

Undertaking studies to gain a better understanding of everyday digital usage

The exploratory analysis of the complaints conducted in this report has opened up a series of avenues that LINC intends to pursue in the coming months. The first aim is to gain a better understanding of the people who turn to the CNIL in order to determine whether socio-economic variables play a role in the implementation of personal data protection rights. At the same time, we would like to undertake a qualitative survey of complainants in order to refine our provisional conclusions on the legal routes taken, to better understand the obstacles encountered and to better accompany individuals,

citizens and consumers on a daily basis. In particular, we wish to consolidate the double-entry analytical framework, mobilising both the stages of recourse to rights as defined in part 4 (making the infrastructure visible, considering oneself a victim and an unbalanced relationship) and the reasons for soliciting and complaining identified in part 3 (blacklisting, marketing, reputation issues and surveillance at work). This would make it possible to identify more clearly the tools that can be used to make these processes less tortuous for the individual.

More generally, the CNIL needs to strengthen its analysis of uses, to better understand how people cope with digital technology and manage the circulation of their personal information in different sectors (education, work, public services, leisure, etc.). A situated understanding of these uses and the logics that guide them is necessary in order to adapt prevention policies and support for individuals in their diversity. This recommendation calls for the development of further empirical work on digital uses and everyday practices with regard to personal data protection.

Expanding our collaboration with researchers

With this in mind, the CNIL, via LINC, will deepen its relations with the research community in an interdisciplinary context. The CNIL's links with academic research are long-standing, taking the form of partnerships (Inria, IMT), or case-by-case collaboration with research teams on projects of common interest. LINC intends to develop its collaborations from 2021 onwards, addressing in particular the tools for making data collection infrastructures visible, the understanding of digital uses and the legal routes taken by individuals.

MAKING THE DATA INFRASTRUCTURE VISIBLE

Producing regulation through reputational incentives *(sunshine regulation)*

Reputational effects are an important lever for compliance[111]. The fear of a negative reputation, affecting user trust and *ultimately* their business model, may lead companies to opt for best practices in personal data protection. Therefore, betting on publicising and making transparent the practices of players so that the general public can draw its own conclusions will have the possible consequence of allowing them to choose to leave a service with bad practices, or to encourage the organisation to change its behaviour. The orders and public sanctions pronounced by the CNIL also contribute to this, beyond the organisations that are implicated by them. At the same time, the CNIL is developing tools within LINC to make the practices of digital players visible, in order to show infrastructures that are sometimes unknown to users. In September 2020, LINC launched a new version of its CookieViz[112] software, a visualisation tool for measuring the impact of cookies and other tracers during online browsing, as well as a visualisation of the interactions between the different players involved in online advertising[113]. A cookie observatory completes the approach, the objective of which is to make the practices of online advertisers visible so that everyone (general public, civil society, media) can have the tools to monitor developments in the sector in real time. Other projects are in the pipeline, such as a project to map personal data files held by the public sector or to analyse data sharing in connected objects.

The CNIL had already proposed this type of regulation in 2014 with the Mobilitics project (highlighting the transmission of data from smartphone applications and the role of the advertising identifier[114]) and, with regard to design practices, in 2019, in particular to highlight and debate deceptive or abusive design practices *(dark patterns)*. In the same way, one could imagine ways of making visible the cases in which people contact the CNIL, marketing, surveillance at work, certain state registers, etc.

All of these actions would have the consequence of taking the subject beyond the walls of the CNIL and into the hands of society as a whole, of equipping intermediary bodies (see

111 Le rôle des incitations réputationnelles dans la régulation, Séminaire du Club des Régulateurs, Université Paris-Dauphine, 18 October 2019, https://chairgovreg.fondation-dauphine.fr/sites/chairgovreg.fondation-dauphine.fr/files/attachments/synthe%CC%80se_191018_0.pdf
112 https://linc.cnil.fr/fr/cookieviz-une-dataviz-en-temps-reel-du-tracking-de-votre-navigation
113 See for example: https://linc.cnil.fr/visualiser-le-web-publicitaire-avec-les-fichiers-adstxt-et-sellersjson
114 https://linc.cnil.fr/sites/default/files/typo/document/Lettre_IP_N-8-Mobilitics.pdf

below), and of supporting the more traditional tools available to the CNIL.

Improving the visibility of the themes of individual complaints received by the CNIL

Each year, the CNIL's annual report, which is freely accessible, includes statistics on the complaints received over the period, with indications of the sectors and cases it has had to deal with. In order to increase the visibility of these annual figures, it could be interesting to develop in parallel more dynamic visualisation tools for these complaints, for example a dashboard accessible on the website, or a data visualisation. In addition, work could be launched to incorporate the analysis grid produced in parts 3 and 4 of this report.

Such highlighting and regular meetings could thus turn these individual complaints into issues that need to be discussed and addressed collectively. The incorporation of anonymised complaint reports (as already exist in the annual reports) would also benefit individuals, facilitating awareness that their individual situation is shared by many and can be corrected. This would allow for the formation of victims' groups that could collectively address these issues and reverse the balance of power between victims and perpetrators. It would also provide civil society (intermediary bodies and associations) and the media with material for action.

Making system flaws visible

The issue of the visibility of data processing, and of the "flaws", is at the heart of the data protection developments proposed since 2018 by the GDPR. Firstly, information and consent obligations have been strengthened to improve data subject awareness of how their personal data are used. New provisions have been introduced such as the obligation to notify data subjects of a data breach in the event of a high risk to them (Art. 34 of the GDPR), the stated aim of which is to make data breaches visible so that individuals can take action. Furthermore, the new obligation to keep a "record of processing activities" has led many organisations, companies and authorities to put in place real data governance to better monitor the data used and avoid inconsistencies. A first step in making these flaws visible was taken with the opening up of data relating to notifications received by the CNIL in order to create indicators or barometers[115]. Work could be undertaken on ways to make it easier for individuals to find out if any of their data has been released or corrupted.

ENCOURAGING THE DEVELOPMENT AND CREATION OF DATA INTERMEDIARIES

The situations that lead individuals to contact the CNIL, as we saw in part 3 of this report, are often based on a form of individual distress in the face of an event or the repetition of an everyday event that they are unable to rid themselves of.

Supporting the consideration of personal data by trade unions

There are a lot of complaints related to surveillance at work, and in particular the use of video surveillance. The COVID-19 pandemic, the various lockdowns and the many people working from home have led to an increase in calls to the CNIL for matters relating to the constant surveillance of employees[116], the use of tracking devices on employee vehicles is multiplying[117], as is biometric access control in the workplace[118] – just a few examples of a field in which there is a great deal of "experimentation" with the rights and freedoms of individuals.

However, the CNIL cannot deal with these issues alone and directly with employees. Although the legal framework allows for a certain number of devices to be put in place, with obligations to inform individuals and the guarantee of GDPR rights, their installation is not compulsory and could be the subject of collective negotiations with employers. The digital world currently lacks intermediary bodies capable of dealing with the issues associated with it: it would be a matter of encouraging traditional trade unions to take greater account of them, but also of seeing the emergence of new forms of trade unions and representative bodies for employees and the self-employed (see box). Historically, it is interesting to note that trade unions have been liaising with the CNIL since its creation[119]. For example, in 1980, the Syndicat de la magistrature, the Confédération syndicale du cadre de vie, the CGT, the CGC, the CFDT and the Fédération des

116 https://www.cnil.fr/fr/les-questions-reponses-de-la-cnil-sur-le-teletravail
117 https://www.cnil.fr/fr/la-geolocalisation-des-vehicules-des-salaries
118 https://www.cnil.fr/fr/biometrie-un-nouveau-cadre-pour-le-controle-dacces-biometrique-sur-les-lieux-de-travail
119 It should also be noted that the CNIL college includes two representatives of the ESEC, one of whom is often from a trade union. 115 Like this one: https://www.pwc.fr/fr/publications/data/barometre-data-breach.html

travailleurs du livre were among the trade union organisations that submitted complaints to the CNIL[120].

Focus on...

Initiatives already exist: the CGT, CFDT, FO and UNSA are already supporting or seeking to support platform workers. New forms of representation are emerging in the UK and Europe around the initiative of the NGO *Worker Info Exchange*, which aims, for example, to help digital workers reclaim their rights over the data collected about them. In the UK, the ADCU (*App Drivers and Couriers Union*) launched a class action in 2020 by Uber and Ola Cabs drivers to demand data access and portability rights in order to produce a "data trust", a pool of data intended to assert their rights with the platforms (which was countered in court in December 2020).

The issue of the use of personal data in the workplace could be the subject of collective bargaining and negotiations, but also of informing certain managers and company directors of their employees' rights. Trade unions and new forms of organisation could also take advantage of Article 77 of the GDPR, which opens up the possibility for collective complaints.

The CNIL could support this movement by producing toolkits for employees, but also for employers who, in the case of the smallest companies, may not comply with the framework simply because they are not aware of it.

Strengthening links with the non-profit world, particularly consumer associations and defenders of public freedoms

Marketing is still one of the most common complaints in 2021. It remains one of the historical reasons why people turn to the CNIL (see box). More broadly, individuals in their status as consumers are faced with the collection and processing of their data on a large scale, by the companies with which they have relations, through the deposit of cookies for advertising purposes, etc.[121]

> *"On several occasions, the Commission has received complaints from individuals complaining of being annoyed by advertising that has reached them at home without their consent, and sometimes, and this is obviously more serious, at their place of work."*
>
> *1978 – 1980, extract from the 1st Annual Report of the CNIL*

The actions carried out by consumer associations on the basis of the collection and processing of personal data correspond to a different and complementary mode, a lever of action to be encouraged in order to enjoin the companies concerned to respect the legal framework, or even to seek compensation[122]. In particular, the CNIL is working with UFC-Que Choisir to integrate the notion of personal data protection into the analysis of products carried out by the latter and published in its magazine.

There are many links between data protection and consumer protection, as shown by the cooperation protocol between the CNIL and the DGCCRF, signed in 2011 and updated in 2019, aimed in particular at "raising consumer awareness and carrying out joint controls". These links, with the regulator and with consumer associations, should be strengthened in order to best meet people's needs.

In addition, the network of associations defending freedoms and human rights – in particular digital freedoms within the European Digital Rights (EDRi) network and, more broadly, those represented within the French National Consultative Commission on Human Rights (CNCDH) – plays a crucial role in making the collection and processing of personal data visible, raising awareness and bringing to light public problems that need to be dealt with by the public authorities.

From the creation of regulatory authorities in the 1970s to the recent decisions of the Court of Justice of the European Union, the mobilisation of civil society has been central to the evolution of personal data regulation, and has contributed to the consideration of these issues in public debate and by the legislator.
These associations can act, as they have already had the opportunity to do, through the use of Article 77 of the GDPR and collective complaints to the CNIL. They also have a role

120 https://www.cnil.fr/sites/default/files/atoms/files/20171116_rapport_annuel_cnil_-_1er_rapport_dactivite_1978-1980_vd.pdf
121 The CNIL devotes a large part of its activities to this type of processing and to the regulation of these sectors, as shown for example by the recommendation on cookies and other tracers published in September 2020, or the sanctions given to Google and Amazon in December 2020.
122 On 7 August 2018, the UFC-Que Choisir association had obtained an order from the Paris High Court (*Tribunal de Grande Instance*) for Twitter to remove more than 250 abusive and/or illicit clauses from its terms of use and its privacy policy. In a judgement of the Paris High Court of 12 February 2019, Google's withdrawal of 209 abusive and illegal clauses, including certain "confidentiality rules". The CNIL had responded to the alert raised by the association in December 2016 about a security flaw in certain connected toys, which had led to a public order being served on the manufacturer of the Cayla doll.

to play – together with the CNIL, and in a different role – in changing mentalities in civil society, public and private organisations, as well as the political field.

Encouraging initiatives of collective and open source production of new technical standards

Faced with the standardisation of digital tools and services offered by the major platforms according to predominantly American standards, individuals concerned about the protection of their data may resort to sometimes rudimentary "tactics" to circumvent them (page 17). While it is necessary to equip individuals so they can digitise and automate these bypasses, the proposal of alternative services and the development of communities of developers and promoters of projects and solutions that are virtuous from the point of view of data protection should be encouraged and supported.

For example, such initiatives are underway in the field of data portability, in order to produce common standards, led by associations and groups of entrepreneurs, partly taken up at European level in the *Data Governance Act*, currently being negotiated by the European Commission. LINC already proposes a 'mapping of tools and privacy protection practices' (see below), but each sector and each type of service could similarly work towards the creation of common standards, different from the de facto standards imposed by the largest platforms (this proposal was already included for design practices in our IP6 report, page 42)[123]. It is also important to encourage and incentivise the technical building blocks that today act as gateways to content or services – browsers, mobile operating systems, social networks – to offer open interfaces and development environments to enable third parties to offer tools, software and extensions that enhance data protection.

The challenge for privacy-protecting solutions and standards remains to scale up in order to benefit from the network effects that will enable them to develop. The example of Signal messaging and the explosion in its user numbers when WhatsApp's terms of use were changed in February 2021 shows that users are willing to test and migrate to new services.

PRODUCING POSITIVE PREVENTION OF DIGITAL USES AND PERSONAL DATA PROTECTION

Not considering the victim as (ir)responsible

To consider victims as responsible is to consider them irresponsible. Protection of private life and data, while touching on privacy, is nonetheless an issue that needs to be debated at the collective level of the organisation of data collection and processing (systems in which individuals are engaged). As discussed in Part 2, page 20, individuals are faced with "multiple micro-decisions that they have to make without the risk to their privacy always being prioritised", which conflict with "other imperatives and interests at stake in the different spheres of their lives, such as work, friendships, family or public life". Everyone has to make choices in how they use digital tools, with the desire not to cut themselves off from their social ties, especially among young people and teenagers. Neither really a victim, nor irresponsible, each person makes his or her choices according to the parameters he or she has to take into account. Prevention should not be about excluding certain digital practices or using certain services.

As such, prevention policies cannot aim to make individuals responsible for the harm they may suffer as a result of the processing of their personal data, or the visibility of their image and profile, for example. As we analyse in Part 2, the empowerment of individuals produces detrimental side-effects: because they feel guilty about their behaviour, victims do not attribute responsibility for their situation to a third party and suffer it rather than engage in a process of enforcing their rights. There is thus a risk in focusing on the individual and his or her practices rather than questioning the institutions and structures that put individuals in problematic situations.

123 https://www.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf

Protecting the context

The importance that the CNIL gives to data protection should not lead to the objective that each individual is fully aware, at all times and in all situations, of his or her rights and of the choices he or she can make. If data protection is often a minor consideration in an individual decision, it is often because individuals want to benefit from 'automatic' protection, which would not depend on their ability to consent or object. The notion of "contextual integrity" developed in this report should be considered more systematically by organisations to limit data processing to operations that are "reasonably expected" by the data subjects and to avoid, as much as possible, uses that are far removed from the context in which the individual is placed.

Particular vigilance must therefore be exercised with regard to the practices put in place by the major digital players over the last twenty years to "standardise" decontextualised practices such as the famous "we process your data to improve our services", the vagueness of which contributes to undermining the importance of context. In this respect, it seems relevant to refer to the notion of *common decency* proposed by George Orwell to characterise the functioning of a democratic society in order to encourage approaches that do not consist of massive, undifferentiated processing of data on individuals without any real reason.

Adapting prevention policies and campaigns

Educational discourse on digital technology is essential to provide knowledge and resources to individuals and professionals. Currently focused mainly on young people and those who are distant from the digital world, lifelong learning opportunities should be strengthened first and foremost, as skills needs are evolving.

Moreover, to be accepted, these messages and campaigns must be adapted to the individuals and anchored in their digital practices through concrete exercises and advice (this requires us to first strengthen our knowledge of digital uses through surveys).

As Anne Cordier laments: *"For example, telling an 8-year-old child that he should be careful about the information he leaves online because his future employer could find out about it makes no sense to him, the world of work is alien to him!"*[124].

To remedy this, it is necessary to start from everyday situations, to invest in different media and to pluralise the messages according to the targets. Finally, rather than making individuals feel guilty by pointing out bad practices, prevention policies would benefit from providing keys to understanding how digital technologies and their ecosystem work.

Making inclusion and data protection education public priorities

Inclusion and education are dimensions of digital policies in France that have proven insufficient, as illustrated by the history of digitisation 'plans' since the 1960s. At local or national level, policies aimed at attractiveness, innovation and economic development have more often met with the interest of decision-makers than those on the daily practices of individuals. Individuals are implicitly seen as empowered to acquire the knowledge and skills necessary for inclusion in our digital society. Digital inequalities are increasing as the Covid-19 health crisis has highlighted.

While new approaches in this area rely primarily on a multitude of public, private and non-profit players, they implement partial solutions, targeting certain audiences, in very disparate ways depending on the territory and promoting various messages, without it being clear who is steering this policy and what its aims are, and without regular national funding being used to consolidate this ecosystem. It is often difficult for individuals to find their way in a shifting landscape of support structures and programmes.

To remedy this, in September 2020 the Secretary of State for Digital Affairs launched a stimulus plan for digital inclusion, with the aim of *"giving digital inclusion an unprecedented boost"*. This plan reinforces the National Plan for Digital Inclusion (September 2018) and aims in particular to *"equip the digital helpers who accompany French people who will never be independent with regard to digital technology"*, by *"expanding the Aidants Connect digital public service and enhancing the digital skills of professional helpers"*, and *"offering training for individuals"*,

124 https://linc.cnil.fr/anne-cordier-la-socialisation-un-effet-majeur-sur-les-pratiques-des-jeunes-en-matiere-de-protection

through 4,000 digital advisers. The design and deployment of accessible and attractive digital inclusion kits for local structures is also part of the project.

The issue of data protection and privacy must be included in this digital inclusion plan. As we have seen (page 24), although the issues addressed by the CNIL are not always a priority for the most digitally illiterate people, they may nevertheless experience problems in their daily lives, particularly in accessing certain services.

People who are far removed from, or not very familiar with, digital technology need to acquire the basics in order to understand their rights and how to assert them. In 2019, the CNIL published an information kit for social workers to protect the data of their clients[125]. In the same vein, the CNIL could work on the definition of recommendations based on the real needs that exchanges with digital inclusion stakeholders might identify.

The digitalisation of the State and the multiplication of new digital services are forcing some non-users of digital technology to confront it, and with them, their helpers and carers. This transition pushes some digital mediators in particular into a position of social rather than digital support. It therefore seems necessary to think about the formation of a mixed support role, which would make it possible to combine access to social benefits with digital skills.

Finally, the focus is often – quite rightly – on the most digitally excluded populations, those without basic digital skills. However, there are a multitude of processes of digital exclusion, of varying degrees of importance, that are part of everyday routines. People who have difficulties with digital technoligies can have rich digital practices.

An individual may be self-sufficient in some things but not at all in others. Digital skills are not equal in themselves: they depend on specific usage situations. Fears and apprehensions about the control of one's own personal data, in particular, are embedded in routine use. For example, online payment is a process that scares a lot of people. Therefore, it would be better to focus on situations rather than profiles, on the hardships faced by individuals rather than categories.

Shaping the imagination: making data protection desirable

To support prevention, develop a culture of risk and make data protection desirable, new imaginations need to be cultivated. Societies are constructed through myths and poetry, as anthropologists have analysed. Imagining, creating and telling stories about the place of digital technology, and in particular personal data, in our societies allows us to project ourselves into the future, both individually and collectively, to discuss it and to put in place the conditions to make it happen – or not.

Looking at the world differently offers perspectives and alternatives. Imagination allows us to rethink our relationship with personal data and to make the invisible visible. With this in mind, LINC has organised a 'fragments of imagination' collection and set up internal creativity workshops. We recommend that these experiments be continued and stepped up in order to build up a collaborative library of imaginations relating to personal data protection. At the same time, the CNIL can play a role in stimulating artistic creation on these themes, for example by organising calls or competitions (short stories, photos, etc.).

Providing tools for empowerment

The Law for a Digital Republic asserts the CNIL's mission to *"promote the use of privacy-protecting technologies, particularly data encryption technologies"*. Without creating confusion with the certification or labelling missions, provided for in particular by Article 42 of the General Data Protection Regulation, the CNIL encourages and shows the different possibilities offered so that each individual is able to adopt "privacy friendly" tools in his or her daily use.

As early as 2017, a tool was launched to make the right to delisting a reality by also allowing individuals to track the progress and effectiveness of their application[126]. In the same year, LINC published a map of privacy protection tools and practices, identifying "tools, services, objects or tricks that individuals can use in their daily lives with the explicit or implicit purpose of protecting their privacy"[127].

125 https://www.cnil.fr/fr/travailleurs-sociaux-un-kit-dinformation-pour-proteger-les-donnees-de-vos-publics
126 https://linc.cnil.fr/fr/outil-controlez-votre-dereferencement
127 https://linc.cnil.fr/fr/une-cartographie-des-outils-et-pratiques-de-protection-de-la-vie-privee

This map can be updated regularly and communicated more widely to individuals.

In the same way, the CNIL will be able, as it has already done, to promote cookie blocking initiatives whose economic model remains virtuous, or any other means enabling people to protect themselves. More generally, while designers of digital services are always looking for greater fluidity, the analysis carried out in this report shows that moments of choice or configuration are particularly important for realising the data collected. Therefore, as we have already recommended in our previous publications[128], we advocate the maintenance of 'desirable frictions', which draw users' attention to data processing.

These tools are not a substitute for the obligation of data controllers to comply with data protection rules, but rather a supplement to them, to empower individuals with informational self-determination.

128 IP report No. 6, *Shaping Choices in the Digital World*; White paper, *À votre écoute*

Focus on...

Global consideration of digital challenges by public services

The receipt by the CNIL of numerous requests that do not fall within its remit and that point to more general issues relating to the use of the web and the various digital services and tools highlights the difficulties in providing guidance and information to the public when they are faced with a problematic situation. The impacts that this absence can have on individuals are not trivial (psychological, moral, financial, etc. – see section 3).

In many cases, the CNIL redirects and guides individuals to other channels of appeal, other institutions, which are competent or expert on specific issues, but illegible or even invisible for people. It therefore seems necessary to be able to clarify these routes for individuals so that, as soon as they are faced with a problematic situation, they know who they should contact to resolve their case. However, in addition to a lack of knowledge of existing remedies, individuals may also find themselves at a loss when they receive a negative response or no response from a channel that has been identified as the solution to their problem (see box on *page 46*). The CNIL then finds itself in the position of having to help prepare certain individuals in their appeal process, in particular by helping to qualify the real nature of the problem in order to guide them correctly.

This dual challenge – while important for the CNIL in the sense that it would make it easier for individuals to make use of their rights and for its staff to devote more time to missions that fall within their remit – goes beyond the institution. There is a more general need for the government to find solutions to these problems, which are rooted at various levels and in various situations. And even more so when the digital transformation of public services and their dematerialisation is accelerating.

Of course, "solving the internet issues" is complex. It requires several types of adjustments and political choices, but it seems important to highlight the recurring problems of the people who come to it. Thus, it seems important to treat more seriously digital complaints, which, as we have seen throughout this report, are not trivial situations. Appeals between individuals concerning private video surveillance (e.g. relating to neighbourhood relations) or the issue of online harassment also represent a significant proportion of the institution's requests. This would involve stepping up the training of officials (including police officers) and giving them the means to investigate illegal content and behaviour online, etc.

The **Foresight** Committee

The CNIL hosts a committee of twenty-one experts with varied backgrounds and profiles to enrich forward thinking and contribute to the debate on digital ethics. Being more attentive and open to the outside world, and working in partnership with the world of research and innovation, these are the objectives pursued by the CNIL with this Committee.

Chaired by the President of the CNIL, **Marie-Laure Denis**, the committee is composed of the following members:

EXTERNAL EXPERTS

Pierre Bellanger,
pioneer of free radio,
entrepreneur and Internet expert.

Pierre-Jean Benghozi,
director of research at the Centre National de la Recherche scientifique (CNRS), professor at the Ecole Polytechnique and professor at the University of Geneva.

Stefana Broadbent,
psychologist, anthropologist, associate professor in the design department of the Politecnico di Milano.

Isabelle Bordry,
entrepreneur, pioneer of the French digital media industry.

Dominique Cardon,
sociologist, scientific director of the Médialab of Sciences Po Paris, member of the editorial board of the *Réseaux* journal.

Milad Doueihi,
philosopher, historian of religions and holder of the chair of digital humanism at the University of Paris-Sorbonne (Paris IV), co-holder of the Collège des Bernardins chair on human challenges of digital culture.

Célia Hodent,
psychologist specialising in the application of user experience in video game design.

Claude Kirchner,
Director of research at Inria,
Director of the Comité national pilote d'éthique du numérique (CNPEN), advisor to the Chairman of Inria.

David Le Breton,
Professor of Sociology and Anthropology at the University of Strasbourg.

Titiou Lecoq,
freelance journalist, blogger, essayist and novelist, specialist in web culture.

Philippe Lemoine,
entrepreneur and essayist, Chairman of the Action-Modernités forum, Chairman of the FING.

Lionel Maurel,
Deputy Scientific Director at the National Institute of Humanities and Social Sciences of the CNRS - InSHS Institute of Human and Social Sciences, author of the S.I.Lex blog on the transformations of law in the digital age.

Cécile Méadel,
sociologist, professor at Panthéon-Assas University, head of the Communication and Multimedia Master's degree.
Researcher at CARISM, Associate Researcher at the Centre for the Sociology of Innovation (Mines-CNRS).

Tristan Nitot,
entrepreneur, author and speaker on the subject of digital freedoms, founded and chaired Mozilla Europe.

Éric Pérès,
Secretary-General of FO-Cadres, member of the Economic, Social and Environmental Council (ESEC).

Antoinette Rouvroy,
lawyer, FNRS researcher at the Centre de Recherche Information, Droit et Société (CRIDS) in Namur.

Henri Verdier,
Digital Ambassador.

Nicolas Vanbremeersch,
entrepreneur, chairman and founder of the Spintank agency and coworking space Le Tank.

Célia Zolynski,
Associate Professor of Private Law at the Sorbonne Law School - University of Paris 1 Panthéon-Sorbonne - Qualified personality at the CNCDH and the CSPLA,
Member of the National Digital Ethics Committee.

MEMBERS OF THE CNIL

Bertrand Du Marais,
Councillor of State.

Valérie Peugeot,
a researcher in the Orange Labs social and human sciences laboratory.

The Innovation and Foresight Reports Collection

Within the CNIL's Technology and Innovation Department, the Innovation, Studies and Foresight team leads research projects and explores emerging topics related to personal data and privacy. Its work lies at the crossroads of innovation, technology, practice, society, regulation and ethics.

The purpose of the Innovation and Foresight IP series of reports is to present and share the work and prospective studies carried out by the CNIL. The aim is to contribute to multidisciplinary and open discussion in the field of Data Protection and to fuel debate on digital ethics subjects.

This is the 8th publication in the collection:

IP REPORT No. 1 - Privacy towards 2020
Expert views

IP REPORT No. 2 - The body as a new connected object
From Quantified Self to M-Health: the new territories of the data world

IP REPORT No. 3 - Data, muses and borders of creative arts
Reading, listening, watching and gaming in the age of personalisation

IP REPORT No. 4 - ed. Foresight Committee: Share!
Motivations and trade-offs for sharing oneself in the digital society

IP REPORT No. 5 - The city as a platform
Personal data at the heart of the smart city

IP REPORT No. 6 - Shaping choices in the digital world
From dark patterns to data protection: the influence of ux/ui design on user empowerment

IP REPORT No. 7 - Civic Tech, data and *Demos*
Issues of personal data and freedoms in the relationship between democracy, technology and citizen participation

You can also find us on the LINC editorial space (http://linc.cnil.fr).

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

April 2021
Commission Nationale de l'Informatique et des Libertés
3, place de Fontenoy
TSA 80715
75334 PARIS CEDEX 07
Tel. +33 (0)1 53 73 22 22
ip@cnil.fr

www.cnil.fr

linc.cnil.fr

LINC
CNIL.