2015

36th Activity Report

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

**TO PROTECT PERSONAL DATA,
SUPPORT INNOVATION,
PRESERVE INDIVIDUAL LIBERTIES**

CNIL
Commission Nationale de l'Informatique et des Libertés

2015 Key figures

Advice and regulation

2 571
DECISIONS ADOPTED
- 122 opinions
- 244 authorisations

1 076
AUTHORISATIONS REGARDING DATA TRANSFERS

Compliance monitoring

96 323
PRIOR NOTIFICATIONS RECEIVED

12 463
PRIOR NOTIFICATIONS REGARDING CCTV SYSTEMS

6 852
PRIOR NOTIFICATIONS REGARDING GEOLOCALISATION DEVICES

359
AUTHORISATIONS REGARDING BIOMETRIC SYSTEMS

73
PRIVACY SEALS DELIVERED

16 406
ORGANISATIONS WITH A DATA PROTECTION OFFICER

Information

136 251
PHONE CALLS RECEIVED

250
SPEECHES FOR CONFERENCES, FAIRS.

Inspections

510 INSPECTIONS

155 ONLINE INSPECTIONS

87 INSPECTIONS REGARDING CCTV SYSTEMS

orders and sanctions

93 ORDERS

10 SANCTIONS
- 3 financial sanctions
- 7 warnings

Protecting citizens

7 908
COMPLAINTS

450
COMPLAINTS following a reject from a search engine of a delisting request

5 890
REQUESTS FOR ACCESS to personal data within police files, surveillance files and FICOBA

36TH ACTIVITY REPORT 2015

Commission Nationale de l'Informatique et des Libertés

INTRODUCTION

1 ANALYSES

2 ACTIVITY REPORT

3 TOPICS OF REFLECTION IN 2016

FOREWORD
BY THE CHAIR

Freedom, no matter what!

Isabelle Falque-Pierrotin,
Présidente de la CNIL

2015: SHOCKED AND STUNNED

2015 began and ended with the violent attacks that plunged France into mourning. There will definitely be a before and an after 2015. Each of us was deeply hurt by the physical violence of these attacks on our democratic values, on what unites us and binds us, and which is the cornerstone of our identity as French and European citizens. These humanistic values hold special meaning for the CNIL's 200 staff members and 17 Commissioners.

> "The CNIL has maintained its course, seeking a delicate balance between disparate but not necessarily antagonistic requirements."

Since then, the cursor between security requirements and the defence of fundamental freedoms has unquestionably shifted. In this very particular context, underscored by intense emotion, the CNIL has maintained its course, seeking a delicate balance between disparate but not necessarily antagonistic requirements.

Over and above their individual and collective impacts, these events have had a very direct impact on the CNIL's activity. The Commission has had to issue opinions on 14 texts (implementing decrees and bills) related to counter-terrorism measures or intelligence. While some of them were already planned, the attacks clearly hastened their implementation.

The final text of the Intelligence Act factored in the various points that the CNIL had drawn attention to in its opinion. And yet, as I have mentioned publicly, the CNIL regrets that intelligence files are not subject to an effective a posteriori inspection of their compliance with the French Data Protection Act *(Loi Informatique et Libertés)*. However, this inspection is a fundamental requirement to establish the files' legitimacy in accordance with citizens' rights and freedoms.

> “The strategic plan is intended to devise a project for the CNIL in an “extraordinary” period full of opportunities and challenges.”

DIn a different register, and proportionally speaking, of course, I would also describe as a shock the decision of the Court of Justice of the European Union on 6 October, declaring the Commission’s **Safe Harbour Decision** invalid. This decision was a real upheaval in Europe and the United States, for businesses, governments, the European Commission and also the data protection authorities.

Basically, the CJEU noted that the United States public authorities can obtain generalised, indiscriminate access to data transferred under the July 2000 *Safe Harbour Decision* without providing effective legal protection to the people concerned. Observing that the Commission had not sought to ascertain whether the United States did indeed “ensure” adequate protection, the Court declared the Safe Harbour Decision invalid. **The issue of generalised and indiscriminate surveillance is therefore central to the CJEU’s invalidation of the Safe Harbour Decision.** This is consistent with the position held by the Article 29 Working Party (Art. WP29), which had deemed that such surveillance was incompatible with the European legal framework and that transfer tools could not be a solution to the problem.

With the WP29’s support and backing, the European authorities immediately assembled to examine the operational consequences of this landmark decision for the protection of European citizens’ data. On 16 October, they asked the Member States and the European institutions to begin talks with the United States authorities, within three months, to find political, legal and technical solutions to enable data to be transferred to the United States without infringing fundamental rights. It became patently clear that the negotiators’ prime concern was the commercial stakes, since they seemed to downplay, if not ignore, the core issue of surveillance, at least initially. It was only a matter of hours before the cutoff date on 31 January that the outline of a new agreement, entitled *Privacy Shield*, was announced.

The WP29 will analyse the new agreement in the light of the essential European safeguards highlighted by the CJEU. It has already made plans to convene an extraordinary plenary meeting next April.

In the case of the Safe Harbour Agreement, the European protection authorities must defend a common European position that is at once firm and pragmatic, in an extremely complex environment with high economic and political stakes. Because the real issue here is to **draw up a global standard that will guarantee European citizens of continuous protection of their data and their rights, even when they leave Europe**.

SO WHAT CAN WE SAY ABOUT 2016

2016 will definitely be a tricky year in which anything could happen. In this unstable context, it is vital to set a course and stick to it because, as we saw in 2015, stability will not come from outside: far from it. And the course set will be the strategic plan for 2016-2018 laid down by the CNIL. Drawing up the strategic plan was a collaborative process in which all CNIL staff members were asked to contribute to the group discussion.

This three-year strategic plan is intended to enable the CNIL to not only pursue the changes already unfolding but also devise a project for a period that we can aptly describe as “extraordinary” in the opportunities and challenges it holds.

The first challenge is to make the transition to the European General Data Protection Regulation and Europeanise certain CNIL activities. The eagerly-awaited European regulation will finally be put to the vote in spring. Its adoption in December 2015 is the result of four years’ hard work and intense negotiation, and marks a major turning point in the regulation of personal data. We will go from a national framework to a primarily European framework. As a result, the CNIL will have to take account of the European aspect of the regulation in everything it does.

▸▸▸

This adoption also signals the beginning of the two-year countdown until the regulation actually takes effect in 2018. The CNIL will have to adjust its procedures, its tools and the role of the plenary session, and also closely supervise the overhaul of the French Data Protection Act, which will still apply for public authorities' files and some health files.

It is a tricky exercise because it entails completely changing the software while still continuing to ensure that the current legal framework is properly applied through to 2018. And yet this transitional period is also an opportunity for the CNIL to update its policy principles, practices and tools.

By establishing joint decision-making power for data protection authorities across the European Union, the regulation makes it necessary to systematise cooperation and information sharing with our counterparts. It also implies cooperation during the upstream compliance stage so that European stakeholders can be given the standardised tools they have been calling for, such as reference standards, privacy seals, compliance packages and so on.

The second challenge the CNIL must tackle is to ground its action in guiding and facilitating business and government stakeholders' digital transition. This transition, though already under way in recent years, will gather pace over the next three years. The CNIL must guide and support the development of trusted digital services with a view to ensuring their compliance and respect for human rights. To do so, it will be more open to the outside world and closer to stakeholders in the field. It will develop a more "mobile" policy principle, along with new, practical tools (self-assessment tools, new privacy seals or reference standards, etc.).

And finally, the last challenge is to make the CNIL the general public's benchmark in digital affairs. One of the CNIL's strengths is its ability to address a community of widely varying audiences, including the general public. More and more citizens are applying directly to the CNIL, which they see as the benchmark public service for digital technology and a trusted partner, as can be seen by the 7,900 complaints received in 2015 (a new record), the 136,000 calls, the 4,385 online queries through the "Need help?" button, whose questions and answers were viewed 122,000 times.

> "The CNIL is ready to undergo changes to become more agile and more pragmatic."

The Digital Republic Bill consolidates the CNIL's role and provides for assigning it the task of organising study and discussion on digital ethics. The purpose of this task is to involve civil society in public debate on the emerging social issues raised by digital technology, looking beyond the framework of personal data as such. The CNIL does not intend to shoulder this new study task on its own. On the contrary, it intends to act as a catalyst for community debate and a community manager.

These are all huge challenges. They illustrate the tremendous changes at work in our society as a result of digital technology.
The CNIL is ready to take up these challenges and it will not do so alone. In a digital world that is complex, abundant, multifaceted and changing, it will share the task of regulation with others, in France and Europe, by developing co-regulation and inter-regulation.

But the questions are not only technical, legal and economic. They do not concern only professionals and experts. The crux of the matter, most of the time, is a vision of society and a choice of values. In this respect, I would like to say that the CNIL is resolutely determined to defend freedoms. In the current context, all CNIL staff members and Commissioners want to work with every sector of society, and boldly and determinedly help establish a digital society that factors in the full diversity of individual needs. ■

1

ANALYSES

What safeguards apply to citizens' personal data in the fight against terrorism?

Personal data protection in the midst of cybersecurity

Invalidation of the Safe Harbour decision: the CNIL and the WP29 working hand-in-hand to factor in the consequences of the Schrems judgement

What safeguards apply to citizens' personal data in the fight against terrorism?

The series of tragic attacks that marked 2015 naturally led the public authorities to wonder about intelligence services' resources and effectiveness. The government took a number of measures designed to bolster intelligence services' means of action, and some of these measures directly concerned privacy and the protection of personal data.

As a result, the CNIL received particularly large numbers of requests during the year concerning these issues and the questions they raise about the way to reconcile security requirements and fundamental freedoms. In a situation such as this, the CNIL's role goes beyond the over-simplistic dichotomy between security and freedoms. Its role is to ensure that the increased means allocated to antiterrorism services are accompanied by real, effective safeguards, which alone are capable of guaranteeing the balance necessary for the "Republican pact" (the principle of equal rights and equal treatment for all) and avoiding any disproportionate infringement of the fundamental right to privacy.

COUNTER-TERRORISM AND PERSONAL DATA PROTECTION: A LONG STORY

A necessary part of combating terrorism is collecting and analysing relevant information, hence data of a personal nature. The legislator has intervened on numerous occasions in this matter, in both the legal and administrative aspects of combating terrorism, to provide the legal safeguards capable of striking a balanced compromise between the objective of maintaining public order, as a constitutional value, and the right to privacy. From the 1980s through to the adoption of the Intelligence Act of 24 July 2015, nearly 20 laws were passed in the matter. One of the most substantial of these is the Act of 10 July 1991 on the secrecy of correspondence transmitted by electronic means. This act created the system of interception for security reasons ("administrative" wiretapping). Other examples include the Counter-Terrorism Act of 23 January 2006 (referred to in France as the "LAT" Act) and the Military Spending Act of 18 December 2013 (the "LPM" Act).

The LAT act gave the intelligence services a wide range of powers. It laid down the basis of a legal framework for administrative requisitions of communi-

cations data; it gave permission for video cameras to be installed in public areas to prevent acts of terrorism; it authorised the authorities to monitor the movements of people likely to take part in a terrorist action, at both national level (automatic number plate recognition systems, or LAPI in French) and international level; it gave the authorities permission to process data collected in connection with international flights.

The LPM act also widened the options available to the "intelligence community" by giving them access to certain administrative and judicial files, by substantially modifying the legal regulations on administrative requisitions of communications data, and by, for example, allowing real-time geolocation of people's mobile devices. It also authorised pilot testing of the "API-PNR France" system, which collects data on airline passengers for use by police officers, gendarmes, customs officers and specialised intelligence services for counter-terrorism purposes.

The CNIL has issued opinions on most of these legislative provisions, along with their regulatory implementation texts. It has therefore been able to examine the proportionality of the various provisions with regard to the right to privacy and communicate its analyses to the authorities. Although not all of these observations were acted upon, a legal framework has gradually been defined for the use of the various personal data files to which intelligence services have access. Its progressive developments also bear witness to the increased means of surveillance made available to the intelligence community in recent years.

A LOOK BACK OVER 2015

2015 stands out for the great number of legislative and regulatory measures adopted concerning the processing of personal data for counter-terrorism purposes, the main ones being the numerous provisions of the Intelligence Act of 24 July 2015.

Moreover, some of the provisions adopted were more extensive than before in terms of the volume of data processed or the collection methods.

Regarding the collection and processing of personal data, **three trends can be observed:**

- the creation of new files for use in combating terrorism, or the modification of certain existing files already used for the purpose;
- the surveillance and monitoring of electronic communications, including the use of new investigation and data collection techniques;
- progress in intelligence, with the ability to collect large volumes of data for the purpose of identifying the people to watch. The Intelligence Act in itself contains all three of these trends.

> **In 2015, the CNIL issued opinions on 14 draft legislative or regulatory provisions directly related to data processing for intelligence or counter-terrorism purposes.**

The creation of new files and the modification of existing files

Following the attacks in January 2015, the government had announced the creation of a new file for tracking people implicated in or convicted of terrorism-related offences. On 7 April 2015, the CNIL issued an opinion on draft legislative provisions aimed at creating a n**ational register of terrorist offenders (named FIJAIT)**, incorporated by amendment into the intelligence bill. The government made this opinion public.

The conditions for using this file are very similar to those for the automated national judiciary register for violent and sex offenders (FIJAISV), on which the Commission has issued opinions on several occasions and which has been examined by both the Conseil Constitutionnel (French Constitutional Council) and the European Court of Human Rights. The aim is to have an address file of terrorist offenders in order to monitor these people by placing various obligations on them (proof of address, of trips abroad, etc.).

Insofar as the safeguards planned for the FIJAIT are identical to those for the FIJAISV, the Commission deemed that they are, in principle, adequate for ensuring a sound balance between respecting privacy and maintaining public order. It nevertheless made several observations aimed at limiting any infringements of fundamental rights and freedoms beyond that strictly necessary. ▸▸▸

For instance, the CNIL remarked that there did not appear to be any point in keeping non-updated addresses, given that the purpose was to monitor the people concerned. Yet addresses were being kept after the date on which these people were no longer under obligation to update them. The same applied to the retention, beyond this date, of data that might already be held in other judicial registers (such as processing previous implications in judicial affairs ("TAJ") and criminal records, for example) or intelligence files (such a CRISTINA). Regarding the recipients of this information, the CNIL deemed that the judicial authorities and the specialised intelligence services should only be able to access the FIJAIT in connection with their counter-terrorism missions. For prefects and government agencies, the scope of the investigations in which data may be disclosed to them should be specified and limited to certain businesses or professions connected to the offences that prompt registration in the file.

LATEST DEVELOPMENT

A decree formally establishes the FIJAIT on 29 December 2015

On 3 December 2015, the CNIL issued an opinion on the draft decree implementing the legislative provisions finally adopted with regard to the FIJAIT. It noted a substantial decrease in the data retention periods and the duration of the obligations incumbent on the people registered in the FIJAIT. At the same time, it pointed out that, for some of the offences concerned, the data retention periods were quite dissimilar to the durations during which the people registered in the FIJAIT were subject to these obligations. The CNIL reminded the authorities that it lay with the minister concerned to take all of the necessary steps to have inaccurate or incomplete data rectified or deleted, under Article 6-4° of the French Data Protection Act.

The new national register of terrorist offenders was finally created by decree on 29 December 2015. Management of this file has been assigned to the national criminal records service, under the authority of the Minister of Justice and under the oversight of a public prosecutor.

In April 2015, the CNIL also examined a data processing operation used by the prison administration to "*track people under criminal justice control, and intended to prevent violations of public safety*" (**known in French as "CAR"**). The CNIL's opinion on the draft decree designed to create the file was not made public because the justice ministry intended to invoke several exemptions that can apply to files involving public safety and State security, laid down in the amended act of 6 January 1978, and more specifically the absence of publication of the said decree and the corresponding CNIL opinion. Nevertheless, it did not exclude this file from the Commission's oversight. This file, which was finally created by a decree dated 10 November 2015 and which is therefore fully subject to CNIL oversight, was approved by the CNIL, but with reservations.

Alongside the creation of these new files, a number of files were modified in 2015.

During parliamentary debate on the Intelligence Act, the government tabled an amendment that would give police and gendarmerie intelligence services access to the **"TAJ" file**, which details **implication in previous criminal cases** and which the CNIL has already examined on numerous occasions. The TAJ file is the judicial history file used by both the French police and the gendarmerie, and which replaced the STIC and JUDEX files, now definitively erased.

The CNIL issued an opinion on the planned legislative provisions on 7 May 2015, then on the implementing decree provided for by the Intelligence Act, on 10 December. As a result, the legal conditions in which specialised intelligence services and services assisting with intelligence tasks can access the TAJ file were substantially modified. For the protection of the nation's fundamental interests, these services can now access the data on all judicial proceedings recorded in the TAJ file, including current proceedings and proceedings for which there is a mention, but excluding data concerning the victims.

The so-called **"FSPRT" file**, which lists people reported for radicalisation of a terrorist nature, has also undergone changes. As with the CAR file, the decrees on this file are not sent for publication, but the CNIL's power to oversee its implementation had not been withdrawn by the government. The CNIL had approved the characteristics of the initial file in late 2014, but was more reticent about the subsequent changes presented to it. It issued a "favourable but with reservations" opinion on the changes, which were set out in the decree dated 30 October 2015.

Lastly, the conditions for using four other files were modified this year in connection with the application of the Act of 13 November 2014, which reinforced counter-terrorism provisions.

This act in fact created provisions prohibiting people from leaving France and excluding people from France. The adoption of these new measures required changes to certain files:

the wanted persons file (FPR), the automated processing of passport-related personal data (TES), processing in relation to secure national identity cards (FNG) and the file of reported objects and vehicles (FOVeS).

The CNIL was asked to examine a draft decree that improved the exchange of information between services for counter-terrorism purposes. The draft decree takes account of the travel restriction provision, which, once applied, invalidates the person's passport and national identity card as a precautionary measure and allows information about these documents to be sent to EU Member States' police authorities. The draft decree would also allow registration in the FPR file of people banned from leaving France and non-French nationals banned from entering France. The CNIL issued an opinion on this decree, published on 15 February 2015, in a deliberation dated 29 January 2015.

The FOVeS file was also modified, by an order of 18 February 2015 based on the CNIL's opinion, to allow decisions by administrative authorities to invalidate documents to be put on record. In the same manner as for the three other files concerned (FPR, TES and FNG), the Commission reiterated the importance of ensuring that the data shown in this file was updated, as soon as possible, to factor in any change in the situation of the people or objects recorded or reported in these files. It is important for the four files concerned to be quickly and effectively updated in order to limit the harmful consequences of retaining people in these files when they no longer met the conditions for being recorded there.

Surveillance of Internet and electronic communications

Citizens' growing use of electronic means of communication and in particular Internet has led the legislator to adopt a number of provisions in recent years concerning the monitoring and surveillance of these means of communication by counter-terrorism services.

The Act No. 2014-1353 of 13 November 2014 reinforcing counter-terrorism provisions authorised the **administrative blocking and delisting of Internet sites that incite or seek to justify acts of terrorism**, adding to an extensive body of counter-terrorism legislation that is regularly expanded and on which the Commission has been able to issue opinions on several occasions.

These administrative measures were clarified by two decrees dated 5 February and 4 March 2015, which were adopted after seeking the CNIL's opinion. As a general rule, they make it possible to involve the technical service providers directly in combating terrorism, and to block or delist websites that are not the subject of a judicial investigation. To guarantee respect for individual freedoms, the Act provides for a qualified person, appointed by the CNIL from among its staff, to ensure the regularity of these various requests and the conditions for establishing, updating, circulating and using the list of websites that have been blocked.

INFO + CNIL

On 29 January, CNIL Commissioner Alexandre Linden was appointed qualified officer in charge of overseeing the new system's implementation. The Trust in the Digital Economy Act, amended by the above-mentioned Act of 13 December 2014, stipulates that this officer is to submit a public activity report each year. This report is separate from the CNIL's annual report.

It deals with the conditions in which it operates and the results obtained, and is submitted to the government and the parliament.

A year earlier, the LPM Act had provided an opportunity to modify the legal regime applicable to administrative access to communications data, in order to give counter-terrorism services broader access to this data.

The Intelligence Act nevertheless marked a turning point in the surveillance of electronic communications. Its primary purpose, as far as the protection of personal data is concerned, was to authorise or legalise **new ways of collecting data travelling over electronic networks, though some were already in use by the intelligence services**.

The creation of several "intelligence collection techniques", now governed by the provisions of the Internal Security Code ("CSI" in French), confirmed the prime importance of surveillance tools to monitor these networks as part of counter-terrorism measures. As the CNIL pointed out in its opinion dated 5 March 2015 on the bill, made public at the request of the Chairperson of the Laws Commission at the National Assembly, these provisions also made it possible to implement far broader surveillance measures than those authorised in recent years.

For instance, the conditions for a **"standard" requisition of communications data** have been modified, substantially extending their retention period by intelligence services: initially kept for one year, then three years under the LPM Act, they can now be kept by these services for five years. **Security interceptions**, i.e. administrative eavesdropping on the content of electronic conversations (phone, e-mail, chat, etc.), have been extended to include people in the circle of family and friends of people under surveillance.

The Intelligence Act also authorised intelligence services to use certain means of surveillance formerly restricted to the judicial police, and authorised the use of new techniques.

▸▸▸

For example, it made provision for **new technical devices that could be used to access computer data** stored in a computer system, that are displayed on a user's computer screen, that the user enters by keying in characters or which are received and sent by audiovisual peripheral devices. Known as "keyloggers", these devices can be used by the judicial authorities in certain proceedings to collect all of the computer data produced or received by a person on his or her electronic terminal.

The provisions of the CSI authorise the installation of **"probes"**, which are used to collect the information processed by the operators concerning a person previously identified as a threat. Information will be collected in real time and directly on request to the network of electronic communications operators.

The provisions also allow intelligence services to install devices at operators' premises that monitor traffic to detect communications likely to represent a terrorist threat. These **"black boxes"** are complex algorithms that, using on predefined criteria, can pick up so-called weak signals that a terrorist act is being prepared.

Intelligence services can also use devices that remotely capture both communications data and the calls exchanged. Known as **"IMSI-catchers"**, these devices are essentially fake mobile towers. They are installed in the vicinity of the target mobile device (at about 100 metres, in the current state of the art) and capture all of the data sent between the electronic device and the real mobile tower.

In its opinion on the bill, the Commission noted that some of the techniques could lead to massive, indiscriminate surveillance of people.

It pointed out that such invasions of privacy, especially concerning the protection of personal data, may be justified by the legitimacy of the objectives pursued and the interests at stake. Moreover, the tools necessary for intelligence services to fulfil their missions must be appropriate for the new forms of action taken by the people and organisations jeopardising these fundamental principles.

Nevertheless, the Commission pointed out that any invasions of privacy must be kept to a strict minimum. They must be appropriate and commensurate with the goal pursued, and adequate safeguards must be in place to govern and oversee their use.

While the CNIL had noted a number of safeguards in the bill submitted to it, it had made numerous additional observations, in particular advocating tighter control of electronic communications surveillance measures. In fact, a number of its proposals have been taken into account and written into the act finally adopted, which is noticeably different from the bill originally submitted to it.

The scale of intelligence has changed: from targeted individual surveillance to a broader focus on people deemed to merit surveillance

Over and above the concrete measures adopted in 2015 by the legislator or the regulator, the Commission observed, in its deliberation on the Intelligence Act, that surveillance measures no longer apply solely to people identified as a terrorist threat. They can also entail the widespread, indiscriminate collection of large volumes of data, among which intelligence services will then have to identify the data relevant to accomplishing their mission.

For example, while the exact conditions for using "black boxes" are not yet known, these tools rest on the assumption that, **to identify the people who represent a threat, intelligence services need to collect and process data for a larger group of people, in this case, the users of electronic communication networks**.

Operators are currently obliged to retain the data sent over their networks so that they can hand it over to the authorities if requested. But with the new provisions for processing data to detect connections, operators will also have to mine the information on all communications matching the parameters established by the intelligence services. These provisions will therefore concern large volumes of data, most of which relate to people who are no threat whatsoever to national security.

These changes must therefore be subject to safeguards that provide effective data protection.

WHAT SAFEGUARDS APPLY TO CITIZENS

The Intelligence Act contains substantial safeguards

In its opinion date 5 March 2015, the CNIL highlighted certain measures designed to curb disproportionate invasions of citizens' privacy. These included defining the scope of intelligence services' activities, their missions, the techniques they can use and the conditions for controlling these measures both beforehand and afterwards. Additional safeguards were subsequently provided as part of the parliamentary debate, adopting some of the recommendations made by the CNIL.

The bill finally adopted was examined by the Conseil constitutionnel, which deemed that, apart from the international surveillance measures and the so-called "operational emergency" procedures, the provisions on intelligence gathering techniques provided adequate controls for the constitutionally-guaranteed principles (right to privacy, freedom of communication and recourse to judicial remedies) and consequently were not a disproportionate violation of these fundamental rights.

These provisions were therefore declared to be in compliance with the constitution, in particular with regard to the following principle safeguards:

- the specific purposes for which each of these techniques can be used - the most intrusive techniques can only be used for some of these purposes;
- compliance with the subsidiarity principle for the use of these techniques, some of which are only authorised when intelligence cannot be gathered by any other means;
- the faculty of adjusting the precise conditions in which the techniques are used, to ensure the proportionality of the measures: with regard to the way the techniques are used and the length of time for which they can be used, the length of time for which the information collected can be used and kept, the locations in which the technical systems can be installed, and the categories of people for whom such measures can be applied (lawyers, members of parliament, etc.);
- the possibility of restricting the use of such techniques to individually named employees specifically accredited for the purpose;
- management control over authorisations to use these techniques, which are issued by the prime minister;
- the oversight exercised by a new, independent administrative authority, the French National Intelligence Techniques Oversight Committee (CNCTR), tasked with examining all authorisation requests for intelligence techniques prior to their use, and with overseeing the use of such techniques;
- the CNCTR's independent status and the effectiveness of its oversight;
- the faculty for any individual to ask the CNCTR and the Conseil d'Etat (French Supreme Administrative Court) to check that no intelligence technique is being used improperly on his or her account.

In so doing, the legislator has brought intelligence techniques under two types of oversight, the first exercised by the CNCTR and the second by the Conseil d'Etat. The new independent administrative authority is responsible for examining the reasons for the intelligence services' request, its purpose, and the proportionality of the use of the technique in question. The Conseil d'Etat is responsible for examining appeals against illegal use of one of the intelligence gathering techniques and can therefore exercise judicial control over these activities.

In practice, citizens can lodge a complaint with the CNCTR when they want to check whether an intelligence technique is being used illegally against them. The CNCTR must then check whether the technique(s) in question have been or are currently used in compliance with the legal framework. If not, it can make recommendations to the relevant authorities.

At the end of this procedure, citizens can also ask the Conseil d'Etat to annul the authorisation to use an intelligence gathering technique, destroy the intelligence collected illegally and pay compensation for the losses sustained.

These safeguards are in addition to those contained in the Data Privacy Act. The information collected with these intelligence gathering techniques is intended to be added to the files used by counter-terrorism services.

The creation and modification of these files are subject to prior examination by the Commission, which has the power to review the conditions in which the majority of these processing operations were carried out. Any person can also apply to the CNIL to exercise their rights to obtain disclosure of and rectify their personal data. The Intelligence Act gave the Conseil d'Etat authority to deal with citizens' applications to exercise their right to access these files.

Lastly, and in a broader perspective, all of the act's provisions must also to be reviewed by the French parliament within five years of the act's implementation.

This periodic review clause will allow the legislator to re-examine the provisions he created in the light of their concrete consequences for citizens. This is a crucial point, in view of the particularly intrusive nature of certain techniques and the emergence of a new principle underlying the intelligence services' action, based on the indiscriminate collection and processing of personal data.

Moreover, within its remit, the CNIL will ensure compliance with the safeguards laid down by the French Data Protection Act. ■

Personal data protection in the midst of cybersecurity

Cybersecurity and privacy can no longer be considered separately. To bolster trust in the digital ecosystem, the CNIL now has a dual role to play: data controllers and the general public need to be helped in building more secure systems and networks, and security best practices have to be promoted in France and abroad.

CYBERSECURITY: A CORE FOCUS OF THE CNIL'S ACTION

2015 was marked by numerous changes in the digital and cybersecurity ecosystem. Cloud computing, Internet of Things and Big Data gained ground; the Act on Military Programming and the Intelligence Act changed the legal landscape; the number of cyberattacks increased again; data hacks became more frequent (Uber, Anthem, Ashley Madison, etc.) and the number of data concerned often ran into tens of millions.

Against this backdrop, how can we build partners' and Internet users' trust to support digital innovation? Efforts to tighten security will have to be not only sustained but also adjusted.

Cybersecurity and privacy must be bound together

Privacy is a key issue in the development of digital technology. The same goes for information security, which underpins infrastructure resilience.

Today, the notions of security and privacy are indissociable. Just as it is inconceivable today to develop a service without taking into account the security aspect, trust in the digital world depends on addressing and upholding the notions of privacy and data protection, as the French Prime Minister reminded listeners during his presentation of the national digital security strategy.

We are still seeing numerous instances of personal data being hacked. These events could have been avoided or at least their impact attenuated by **establishing and following basic security rules**. While it is generally agreed that there is no such thing as absolute

> Privacy is a key issue in the development of digital technology

INFO +

Baseline security rules

- Install security solutions for data traffic and stored data;
- Segregation of different environments, depending on their sensitivity and the data that is processed there (for example, the WiFi network that is open to customers must not be connected to the organisation's back-office or production network);
- Manage permissions to restrict data access to authorised people only, and make security contractual in third-party relations.

security, it seems inconceivable that this most elementary level of security is not respected.

The devices that surround us are becoming increasingly autonomous and smart, and are processing ever-growing volumes of data. Cybercrime is growing too. No longer targeting only big business, it has set its sights on small organisations and even individuals. The pervasiveness of cybercrime on the Internet calls for the use of increasingly sophisticated security solutions to detect frauds and hacks, without infringing on privacy. **Detection is becoming a fundamental part of protecting businesses**, institutions and users in general.

As a result, in the interests of the digital ecosystem and the people who compose it, **rules for openness and information must be established, based on these new security solutions**. The latter must be used to guarantee the protection of the individuals behind the data.

The CNIL's role in cybersecurity

▸ The CNIL helps to build trust in the digital environment. Under Article 34 of the French Data Protection Act, it is tasked with ensuring that entities that process personal data do so in optimal security conditions. It is tackling this task through several initiatives. Through its missions (advice, formalities, controls and sanctions), the CNIL oversees the level of security applied by organisations in systems and networks. It also guides developments in the legal framework through its involvement in the debate on the General Data Protection Regulation (GDPR), the Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS) and the Act for a Digital Republic. It actively participates in a number of specialised information security working groups composed of experts from a variety of backgrounds (Club EBIOS, Club des experts de la sécurité de l'information et du numérique). It also plays a very active role in awareness raising, mainly through its educational initiatives in digital technology.

▸ The CNIL offers technical solutions for data controllers and the general public. In the security field, it publishes guides, information sheets and recommendations to help organisations and citizens adopt best practices and protect themselves from risks. It reviews the security measures applied by data controllers and gives them advice and help with decision making. It is also developing certification for procedures and products, such as digital safes and governance.

▸ The CNIL assists victims of "cyber-malevolence". The CNIL collects complaints in every field related to new technologies and assists victims of cyber-attacks, for example by referring them to the relevant services (police or public prosecutor's department). It also receives notifications of personal data breaches, so that it can then inform the data subjects and take the necessary steps. It also works in partnership with Signal Spam and can inspect companies identified by Signal Spam.

▸ The CNIL champions France's values within the WP29 and other international bodies that work on security and new technologies (OECD, ISO, Berlin Group, International Data Protection and Privacy Commissioners Conference). It edited the main information security standard at ISO (ISO/IEC 27001), contributed to European work on defining security measures for smart grids, represented the WP29 in the Permanent Stakeholders Group advising the ENISA (European Union Agency for Network and Information Security), and provided technical recommendations, at national or European level, in various domains related to new technologies (cloud computing, Internet of Things, etc.). It also acts as regulator for the major Internet players, thereby promoting European values. ▸▸▸

> Addressing security must be a core concern so that we can protect citizens, customers, companies and the digital ecosystem as a whole.

Towards privacy by design

Security must be built into a project right from the start and follow the whole data lifecycle. The same holds for privacy.

It involves a dialogue between the business units and the IT department, and a mutual understanding of the issues at stake in these developments.

Ideally, privacy should be thought out and planned as early as possible, right from the project design stage (hence the notion of *"privacy by design"*).

THE PRIVACY IMPACT ASSESSMENT: A NEW TOOL FOR BUILDING AND DEMONSTRATING COMPLIANCE

To help micro, small and medium-sized enterprises to "take all useful precautions, with regard to the nature of the data and the risks of the processing, to preserve the security of the data" (Article 34 of the French Data Protection Act), the CNIL published an initial guide in 2010 on personal data security. The guide presents the basic precautions to take to ensure that data is processed securely.

In June 2012, the CNIL published an online guide to privacy risk management for complex or high-risk processing operations. This guide aimed to help data controllers form an objective view of the risks generated by their processing operations, and choose the necessary, adequate security measures.

The guide has since been revised to align it more closely on the proposed European Commission General Data Protection Regulation and the work of the WP29 on using a risk-based approach to determine security measures. It also factors in feedback and improvements suggested by various stakeholders. Lastly, it clearly marks the shift from merely applying security best practices to achieving effective, overall compliance with the Data Protection Act.

Since July 2015, the Commission has been publicising its method for conducting Privacy Impact Assessments (PIA) and, in the proposed European Commission General Data Protection Regulation, Data Protection Impact Assessments (DPIA).

Issues involved in risk management and PIAs

In the field of privacy protection, compliance is based mainly on legal requirements. **The principle of security, on the other hand, involves risk management**.

Article 17 of the Data Protection Directive 95/46/EC states that *"the controller must implement [...] measures to [...] ensure a* ***level of security appropriate to the risks represented by the processing and the nature of the data to be protected****"*.

Additionally, Article 34 of the French Data Protection Act states that ***"the data controller shall take all useful precautions, with regard to the nature of the data and the risks of the processing****, to preserve the security of the data"*.

Moreover, Article 33 of the General Data Protection Regulation introduces the obligation to carry out an impact assessment when a processing operation presents a risk to the person's privacy, before undertaking the processing.

Security compliance is based on an assessment of the risks on privacy (who, what?), and not on the mere comparison with best practices or on the mere application of the policy principle (which principle?).

On the other hand, the tools, measures and documentation required (produced in accordance with the accountability principle) can vary with the risks to which the processing operation is exposed.

Thus, the very fact of conducting a PIA, consulting the Data Protection Authority beforehand or taking specific measures to treat the data security risks depends on the level of risk to the processing operation.

What is a PIA?

A step ahead of the proposed European Commission General Data Protection Regulation, **the CNIL published its method for conducting Privacy Impact Assessments (PIAs)**.

Article 33 of the General Data Protection Regulation describes the DPIA as follows:

"The assessment shall contain at least **a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller, an assessment of the necessity and proportionality of the processing operations in relation to the purposes, an assessment of the risks to the rights and freedoms of data subjects and the measures envisaged to address the risks***, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned."*

What do the PIA Manuals contain?

The PIA Manuals are methodological handbooks. The CNIL's method was designed in compliance with the General Data Protection Regulation and international standards. It consists of three manuals:

- PIA Manual 1: **the method;**
- PIA Manual 2: **the tools;**
- PIA Manual 3: **the catalogue of best practices.**

This method is based on two main components:

- **the fundamental principles and rights**, which are "non-negotiable", laid down by law and must be upheld. They cannot be modified at all, whatever the type, severity or likelihood of the risks incurred;
- **management of the privacy risks on data subjects**, which allows determining the appropriate technical and organizational measures to protect their personal data.

The procedure (PIA Manual 1) consists of four steps:

1. **Study the context:** define and describe the processing operations under consideration, their context and the stakes involved;

2. **Study the measures:** identify the existing or planned measures (to meet the legal requirements and also to treat the privacy risks);
3. **Study the risks:** assess the risks to data security and which might have repercussions on the privacy of the data subjects, to ensure that they are being dealt with in a proportionate manner;
4. **Validate:** validate the manner in which the organization plans to meet the legal requirements and treat the risks, in the light of the stakes identified in step 1, or repeat the previous steps.

The tools (PIA Manual 2) contain examples and templates designed to help those conducting a PIA carry out their study and document their report.

- The examples form a knowledge base on all the useful information for carrying out a PIA (sources of risk, impacts on privacy, exploitable threats and vulnerabilities, etc.);
- The manual also contains table and templates for presenting the results of every step of the method.

Lastly, **the catalogue of best practices (PIA Manual 3) provides examples of measures to take** to meet the legal requirements and also to treat the identified risks by using the method. ■

INFO +

The PIA

The PIA is an assessment comprised of a description of the personal data processing operation, an assessment of the risks to privacy, and a description of how the risks will be treated. It applies the privacy risk management process to determine the security measures to be taken.

For cases not covered by compliance packages, simplified formalities or sector-specific guides, and in addition to the latter, the PIA helps achieving compliance, in particular for processing operations that are complex, deemed to be risky or represent high stakes from a data protection and privacy viewpoint.

Invalidation of the Safe Harbour decision: the CNIL and the WP29 working hand-in-hand to factor in the consequences of the Schrems judgement

Edward Snowden's revelations in June 2013 sparked a debate on the extent of the surveillance activities conducted by intelligence services in both the United States and the European Union. The debate focused on the consequences of mass surveillance on privacy and data protection rights.

The facts

Mr Maximillian Schrems, who is an Austrian national, has been using Facebook since 2008. The data that Mr Schrems - or any other Facebook subscriber residing in the European Union - provides to Facebook is transferred, in whole or in part, from Facebook's Irish subsidiary to servers located in the United States, where it is processed.

Mr Schrems filed a complaint with the Irish data protection authority, claiming that, in view of the revelations made in 2013 by Mr Edward Snowden concerning the activities of intelligence services in the United States (and in particular the National Security Agency, or NSA), the law and practices in the United States did not provide sufficient protection against surveillance by the public authorities of data transferred to the United States.

The Irish authority rejected the complaint on the grounds that, in its decision dated 26 July 2002, the Commission had deemed that, within the so-called Safe Harbour regime, the United States provides an adequate level of protection for the personal data transferred there.

The matter was referred to *the High Court of Ireland*, which sought to ascertain whether the Commission's decision effectively prevented a national control authority from investigating a complaint alleging that a third country was not providing an adequate level of protection and, if necessary, suspending the disputed data transfer.

The issue of generalised and indiscriminate surveillance is central to the CJEU's decision.

THE JUDGEMENT HANDED DOWN BY THE COURT OF JUSTICE OF THE EUROPEAN UNION

The judgement[1] handed down by the Court of Justice of the European Union (hereinafter: "CJEU") in the Schrems case **is of major importance for data protection** on a number of accounts.

First of all, the Court replied to the High Court of Ireland that *"**the existence of a Commission decision** finding that a third country ensures an adequate level of protection of the personal data transferred **cannot eliminate or even reduce the powers available to the national supervisory authorities** under the Charter of Fundamental Rights of the European Union and the directive"*.

It added that, **even if the Commission has adopted a decision, the national supervisory authorities**, when dealing with a claim, **must be able to examine, with complete independence, whether the transfer of a person's data to a third country complies with the requirements laid down by the directive**. It therefore confirmed the data protection authorities' independence from the European Commission.

> It therefore confirmed the data protection authorities' independence from the European Commission.

However, the Court alone has jurisdiction to declare whether a Commission decision is valid or not. On this account, it has, through the Schrems judgement, invalidated the decision by which the European Commission had observed that the Safe Harbour principles ensured an adequate level of protection of the European personal data transferred[2].

The Court noted that the Commission had not provided sufficient details in its decision concerning the measures by which the United States ensures an adequate level of protection of the data on account of their national legislation or their international commitments[3].

Indeed, "the protection of the fundamental right to privacy at European Union level requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (Digital Rights Ireland and Others Judgement, Case 293/12 and Case 594/12, EU:C:2014:238, paragraph 52 and the case-law cited)"[4] .

The proportionality requirement

"Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail (see, to this effect, concerning Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54), judgement in Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 57 to 61).""[5]

> The Commission had not provided sufficient details in its decision concerning the measures by which the United States ensures an adequate level of protection of the data.

Generalised access by the public authorities is an infringement of the fundamental right to privacy

"In particular, legislation permitting the public authorities to have access ▸▸▸

1 JUDGMENT OF THE COURT (Grand Chamber), 6 October 2015, in Case C-362/14, request for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 17 July 2014, received at the Court on 25 July 2014, in the proceedings Maximillian Schrems v Data Protection Commissioner, joined party: Digital Rights Ireland Ltd.
2 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [notified under document number C(2000) 2441] (Text with EEA relevance.).
3 See in particular paragraph 83 of the judgement: Decision 2000/520 "concerns only the adequacy of protection provided in the United States under the [Safe Harbour] Principles implemented in accordance with the FAQs with a view to meeting the requirements of Article 25(1) of Directive 95/46/EC," though without containing adequate observations as to the measures by which the United States of America ensures an adequate level of protection, as defined by Article 25, paragraph 6 of this directive, because of their domestic legislation or their international commitments."
4 Paragraph 92 of the Schrems judgement.
5 Paragraph 93 of the Schrems judgement

on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter (see, to this effect, judgement in Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraph 39).[6]

The necessity of an effective means of appeal for people subject to trial

"Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law (see, to this effect, judgements in Les Verts v Parliament, 294/83, EU:C:1986:166, paragraph 23; Johnston, 222/84, EU:C:1986:206, paragraphs 18 and 19; Heylens and Others, 222/86, EU:C:1987:442, paragraph 14; and UGT-Rioja and Others, C-428/06 to C-434/06, EU:C:2008:488, paragraph 80)."

However, "the Commission found that the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security. Also, the Commission noted that the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased."[7]

6 Paragraph 94 of the SCHEMS judgement
7 See paragraph 90 of the judgement.

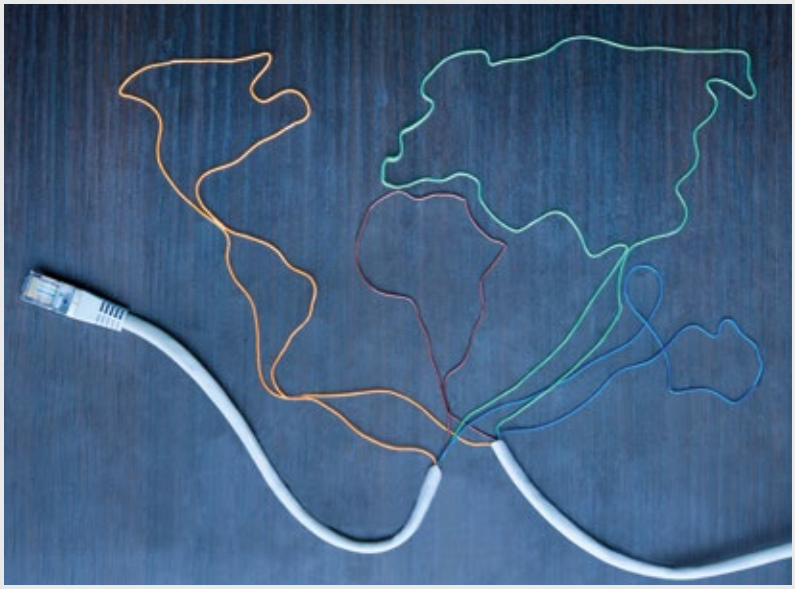
ACTION BY THE WP29

The CNIL and its European counterparts met on 15 October to draw up a joint action plan to help the stakeholders adjust to the new legal context.

On 16 October 2015, the WP29 issued a statement stressing the importance of a combined initiative to manage the judgement's consequences. It also observed that mass surveillance was a decisive factor in the court's reasoning. It recalled its unwavering policy principles, whereby mass surveillance is incompatible with European law, and data transfer tools should not be misused for this purpose.

It called on the European institutions to open discussions with US authorities in order to find legal and technical solutions enabling data transfers to the United States that respect fundamental rights.

In this respect, it considered that the negotiation of an international agreement providing more substantial guarantees for the people concerned could be part of the solution, as could discussions on the reform of the Safe Harbour agreement.



The date of 31 January 2016 was set as a deadline.

The WP29 noted that transfers made under the Safe Harbour decision were unlawful. It then undertook to study the judgement's consequences on the other transfer tools during the time necessary for these talks. It said that the standard contractual clauses and binding corporate rules remained workable during this period, and that the authorities reserved the prerogative to examine specific cases, such as complaints, and exercise their powers to protect individuals' rights. Moreover, the WP29 said that it may take legal action, if necessary, once the allotted time was up.

It also announced awareness-raising initiatives for the stakeholders concerned, encouraging them to reflect on the eventual risks they take when transferring data and consider legal and technical solutions to mitigate those risks.

THE ANALYSIS CARRIED OUT BY THE WP29

In mid-October 2015, the WP29 undertook to analyse the impact of the Schrems judgement and the principles raised by the Court with regard to the other tools for transferring data to third countries, such as standard contractual clauses and binding corporate rules.

To this end, it identified the essential safeguards applicable to intelligence services' activities under the terms of the legal framework and European case law.

It then analysed the legal framework for the activities of the United States' federal intelligence services, and their practices in the light of these safeguards, with a view to checking whether the conditions in which interferences in privacy and data protection are permitted, respect these safeguards.

To corroborate the accuracy of its observations, the WP29 held hearings and consultations of academics, representatives of the private sector and business, US government representatives, and representatives of US and European civil society.

Identifying the essential safeguards applicable to intelligence services' activities under the terms of the legal framework and European case law

Based on the CJEU's observations in the Schrems judgement, the WP29 analysed the Luxembourg Court's other judgements on state surveillance activities, along with the judgements handed down by the European Court of Human Rights (hereinafter: "ECHR") and the primary and secondary law applicable in the matter.

The results of this analysis were discussed at a plenary meeting of the WP29 on 2 and 3 February 2016.

Four essential guarantees apply to intelligence activities:

1. Processing should be based on clear, precise and accessible rules: this means that anyone who is reasonably informed should be able to foresee what might happen with her or his data if it is transferred.

2. The State must be able to demonstrate the necessity and proportionality of its intelligence activities and, more specifically, of the ensuing processing of personal data, with regard to the legitimate objective pursued: a balance needs to be found between the objective for which the data is collected and accessed (generally national security) and the rights of the individual.

3. An independent oversight mechanism should exist, that is both effective and impartial: this can either be a judge or another independent body, as long as it has sufficient ability to carry out the necessary checks.

4. Effective remedies need to be available to the individual: anyone should have the right to defend his or her rights before an independent body.

The WP29 stresses that these four guarantees should be respected whenever personal data is transferred from the EU to the United States and to other third countries, as well as by EU Member States.

Analysis of the legal framework and of United States practices in the light of these essential guaranteess

The WP29 studied the main texts regulating the activities of the United States federal intelligence services and approached the above-mentioned stakeholders for information about their practical application. This analysis and the input from the stakeholders concerned show that the United States made considerable efforts in 2014 and 2015 to provide greater protection for non-US nationals' personal data in this context. However, the WP29 remains concerned about the legal framework currently applicable to the four above-mentioned guarantees, and more specifically their scope and the remedies available to people concerned by the transfer of their personal data from the European Union.

> The WP29 underlined that four essential guarantees applied to US intelligence activities when they collect European citizens' data.

ACTION TAKEN BY THE CNIL

Since the CJEU ruling invalidated the Safe Harbour mechanism that allowed data to be transferred to signatory companies in the United States, it has not been possible to carry out such transfers under Safe Harbour principles.

In formal terms, this means that the companies concerned have to send the CNIL a request to modify their initial declaration, and notify the CNIL that they are either ceasing the transfers in question or using a different tool to oversee the transfers.

The CNIL therefore took steps to inform the companies concerned, advise them of the alternatives available and the procedures for complying with them. More specifically, it sent e-mails to the companies concerned and published questions and answers on its website.

Should data transfers be necessary, and given that the WP29 had deemed that companies could continue using the other legal mechanisms for transfers up until 31 January, the CNIL informed companies of the possibility of using the Binding Corporate Rules[8] and model contract clauses[9] adopted by the European Commission (clauses for transfers from processing managers to processing managers, and clauses for transfers from processing managers to contractors). ■

LAST MINUTE

Announcement of a new Privacy Shield agreement

On 1 February 2016, the United States and the European Commission announced the conclusion of a new agreement, known as the EU-U.S. Privacy Shield. The WP29 must now analyse the agreement's content in depth and assess whether it addresses the major concerns regarding international data transfers raised by the CJEU's ruling. A plenary meeting of the WP29 is scheduled in April 2016.

8 Binding Corporate Rules (BCRs) are a code of conduct setting out a company's policy on data transfers. BCRs provide adequate protection for intra-group data transfers from the European Union to EU third countries.

9 European Commission-approved model contract clauses can be used to govern transfers of personal data outside the European Union. They are designed to ease the task of processing managers when they implement transfer contracts.
A distinction is made between transfers from a processing manager to a processing manager, and transfers from a processing manager to a contractor. There are therefore two types of clauses, one for each type of transfer.

2

ACTIVITY REPORT

International regulation, a vital factor in protecting data in the digital age

International regulation, a vital factor in protecting data in the digital age

2015, FRUITION

In last year's annual report, the CNIL described 2014 as "an emergent year" for the proposed European regulation; 2015 is undoubtedly the year of its fruition. The data protection reform was adopted in December, paving the way for a harmonised adaptation of European law to the digital world.

This outcome was the fruit of hard work by the three EU institutions (the Commission, the Parliament and the Council of the European Union) throughout 2015. An agreement on the regulation was concluded in June, then, in parallel to the trilogue on the regulation, another agreement was reached in October on the draft directive for the police and criminal justice sector. The three institutions reached a common, overall agreement on both texts in a tight timeframe in the second half of the year, officially confirming the new legal framework for data protection in the European Union.

This reform goes far beyond the current directive because the two texts adopted cover processing operations not only in the private sector and the public sector but also those conducted by the police and the criminal justice sector in cooperation.

Now there remains one last, formal step to accomplish: **the adoption of the data protection package in a plenary session of the European Parliament and in the Conseil des ministres, scheduled for spring 2016**.

The CNIL and all of the national data protection authorities have regularly contributed to finalising this draft by publishing their positions at various points in the negotiations. Numerous meetings have also been held to present them to the institutions.

This major turning point represents progress for individual rights, a more effective approach to compliance for businesses, and a new governance model for the authorities.

The challenge now is to turn the text into an operational reality for both processing managers and citizens. This is why, as soon the text's adoption was announced, the WP29 decided on an ambitious action plan to implement the regulation and turn the working party into the European Data Protection Board.

The second high point of the CNIL's international activity in 2015 sprang from the judgement of the European Court of Justice on 6 October 2015 invalidating the Safe Harbour. The WP29 convened an extraordinary plenary meeting on 16 October, at which it called on the European and American institutions and governments to find a solution, by the end of January 2016, to ensure that transfers to the United States were carried out in compliance with European fundamental rights. The WP29 also began an extensive programme of work to assess the judgement's impact on the other data transfer tools, namely the binding corporate rules and the model contract clauses.

2016 promises to hold numerous developments on both the European and the international fronts. A new world is opening for Europe; it must be constructed collectively with civil society stakeholders, industry representatives, institutions and the authorities. Implementing this judgement and the new European regulation is a challenge for everyone and Europe will only be credible and powerful in defending its values if its action is united and coordinated. This is the objective set by the CNIL, which is chairing the WP29 for another two years, and its European counterparts.

> **Europe will only be credible and powerful in defending its values if its action is united and coordinated.**

MONITORING AND FINALISATION OF THE EUROPEAN REFORM

The Regulation

After more than four years of negotiations, 2015 was marked by a twofold political agreement. In June 2015, the Council of the European Union approved an agreement opening the phase of negotiations, or "trilogue", between the three European institutions (the Commission, the Parliament and the Council of the European Union). These negotiations subsequently resulted in an agreement on the text in December 2015.

The latter has yet to be formally adopted by the European institutions, but this approval is a key step, eagerly awaited by all of the stakeholders. The text adopted in December contains the following provisions:

- **For citizens,** their existing rights will be reinforced. Citizens will be able to obtain additional information about how their data is processed, and in a clear, accessible, readily understandable form. The right to be forgotten is consolidated and a new right - the right to portability - is introduced, giving citizens greater control over their data. Special protection is also provided for minors.
- **For companies,** the formalities are simpler and there is the possibility of a single contact person for all European data protection authorities. A compliance toolkit is also made available, containing some new tools (e.g. code of conduct, certification). It will be possible to adapt these tools to the level of risk to individuals' rights and freedoms (e.g. keep a register, consult data protection authorities, report security loopholes, etc.).
- **For data protection authorities**, a declaration of competence as soon as there is an establishment on their territory or their citizens are affected by data processing. They will also be given increased powers, including coercive measures and the ability to impose administrative fines of up to 4% of the global revenues of the company concerned. Most importantly, the CNIL's European counterparts will now be able to make joint decisions, whether they are noting an organisation's compliance or applying a penalty. An integrated Europe will provide greater protection for people and legal security for businesses.
- **Cooperation among data protection authorities will be reorganised and include a new European body:** the European Data Protection Board (EDPB), in charge of arbitrating disagreements between authorities and also drawing up a set of "European" policy principles.

The WP29 monitored these advances closely and contributed its expertise, primarily through regular, joint position statements and meetings with EC institutions.

During the trilogue, for instance, the WP29 indicated in June 2015 the points to which special attention should be paid, specifically:

- The assurance that the new regulatory framework **will not lower the current level of protection** nor challenge the fundamental principles and rights currently set out in Directive 95/46/EC.
- **The broad sense in which personal data should be understood**. For instance, IP addresses and other online identifiers should, as a general rule, be considered personal data.
- **The use of pseudonymisation** as a technique to limit risks for the people concerned. Pseudonyms or pseudonymised data must not be defined as a new category of data that can be used to waive certain obligations defined by the regulation. Pseudonymisation is a security measure only.
- **The need to uphold the founding principles of the purpose and compatibility of processing operations,** especially in the context of big data.
- **Effective protection of the rights of the people concerned,** in particular through an effective right to portability, and data protection authorities endowed with appropriate coercive powers and sufficient resources.
- **A new efficient, balanced, European governance model** for data protection authorities, underpinned by closer relations with citizens and greater cooperation among authorities.

In September 2015, the WP29 also voiced its opinions on the **future internal structure of the EDPB,** considering the following features as essential components of the new European model:

- **A strong, independent EDPB, acting as a key decision-maker.** It is made up of a chairperson, 28 data protection authority commissioners from each Member State and the European data protection controller (tasked with checking that the EC institutions' processing operations are in compliance). It is backed by working groups composed of experts.
- **A Chairperson, appointed by the EDPB, who speaks on behalf of the data protection authorities.** The Chairperson is elected from among the EDPB's members. The Chairperson's term of office must be long enough for the Chair to accomplish his or her missions. To meet this requirement, the Chairperson needs to carry out his or her missions on a full-time basis. The Chairperson, as head of the EDPB, should also have control over his or her budget and staff.
- **An executive committee, whose primary mission is to ensure that the EDPB effectively fulfils its missions.** Composed of the Chairperson and two vice-chairs, it should also help and assist the Chairperson in his or her dealings with the data protection authorities.
- **A secretariat, with sufficient, professional resources.** Provided by the European data protection controller, it is under the responsibility of the EDPB Chairperson.

THE DIRECTIVE

2015 was marked by the completion of the phase of negotiations, or "trilogue"[1] between the three European institutions (the Commission, the Parliament and the Council of the European Union) in December 2015. The parties negotiated the text of the directive on the protection of physical persons with regard to the processing of personal data by the competent authorities for the purposes of preventing and detecting criminal offences, conducting investigations and prosecutions in the matter, or implementing penal sanctions.

The directive has yet to be formally adopted by the European institutions, but the agreement on the text comes almost simultaneously with the agreement on the draft data protect regulation, and accedes to the data protection authorities' request to treat these two texts as a "package".

1 **The European Parliament adopted its position at the first reading on 12 March 2014. The Council released a general guideline on 8 October 2015. Five trilogues then took place from October to 15 December 2015. They resulted in the adoption of the trilogue's text on 16 December 2015 by the Council Member States' Permanent Representatives Committee, and a vote on the text by the European Parliament's Civil Liberties, Justice and Home Affairs Committee on 17 December 2015.**

Limited compliance with the WP29's recommendations

In December 2015, the WP29 wrote to the European institutions to draw attention to some areas of particular concern that needed further attention.

It began by making two general remarks. It regretted the very principle of having two instruments instead of opting for a regulation that applied to all sectors. Many government agencies (taxation, customs, etc.) would have to fulfil different obligations, depending on whether their activities are governed by one or other of the texts. It recalled the current reform's objective of according a high level of protection to data, and consequently insisted that exceptions to the principles on the grounds of the specific features of law enforcement activities should be interpreted narrowly. It also expressed a wish that the principles enshrined in the two texts be set out in a common definition.

It then expressed a number of specific concerns, many of which were dealt with in the text of the agreement reached by the institutions.

Thus, as requested by the WP29, the text of the agreement includes **the definitions of the key concept**s (personal data, processing, pseudonymisation, personal data breach, genetic data, biometric data, health data) laid down by the regulation. In addition, **it differentiates the levels of implication and the roles of the people whose data is processed in the prosecution of criminal offences** (victim, suspect, perpetrator) and ensures the accuracy and relevance of the data processed, and the upholding of the rights associated with these various statuses.

As advocated by the WP29 in its opinions on the data protection reform, processing operations performed for law enforcement purposes will, in the future, have to factor in privacy right from the beginning *(privacy by design) and allow privacy by default*.

In terms of security, the obligations of processing managers and contractors have been reinforced as requested by the WP29: mandatory logging of processing operations, availability to supervisory authorities, with which they must cooperate on request, conduct of a data protection impact study for any processing operation likely to generate a high risk for individuals' rights and freedoms. Moreover, security breaches affecting the personal data processed are to be reported to the supervisory authority as a matter of principle, unless it is unlikely that the breach in question generates risks for an individual's rights and freedoms.

It has become mandatory to appoint a data protection officer, except for courts and other independent judicial authorities.

The text also provides for **the appointment of an independent supervisory authority** to oversee the proper application of the directive and cooperation among the authorities. The WP29 had stressed the particularly important role of these authorities wherever the data processed is used to curb the fundamental freedoms of the individuals concerned on the grounds of preventing, punishing or prosecuting an offence. It would have been preferable, though, to give the supervisory authorities greater powers and increase the penalties applicable for shortcomings.

In its address to the three institutions, the WP29 had appealed to them not to render the key data protection principles ineffectual by allowing too many exceptions. In this respect, the text of the agreement is not entirely satisfactory. For instance, the processing of specific categories of personal data[2] is authorised under certain conditions, instead of being prohibited except in exceptional cases. Likewise, it is possible to make a decision based solely on an automated processing operation, including profiling, if EU law or national law authorises it, whereas the WP29 also recommended prohibiting this except in specific, exceptional circumstances. Moreover, the consultation of the supervisory authority prior to processing is limited to certain cases of processing deemed to be "high risk". Data subjects' rights to access, rectify and erase their data are largely copied on those provided by the regulation, but the situations in which they can be limited or excluded remain vague and could cover a range of scenarios.

The issue of transfers to countries that do not ensure an adequate level of protection also raises some concerns. As the WP29 had pointed out, the question of the purposes for which the data could subsequently be used remains crucial. The issue of mass surveillance should not be side-stepped and data should only be transferred when it is strictly necessary for an investigation or proceedings.

> The WP29 had appealed to render the key data protection principles ineffectual by allowing too many exceptions.

2 Teerm now used to refer to data that reveals racial or ethnic origins, political opinions, religious or philosophical beliefs or trade union affiliation, as well as the processing of genetic data, biometric data capable of identifying a person uniquely, or data concerning the person's health, sex life or sexual orientations.

ART. WP29 CHAIRMANSHIP AND ACTIVITIES

ARTICLE 29
Data Protection Working Party

The WP29, which has been chaired by the CNIL Chairwoman since February 2014, decided to make its positions clear on fundamental issues such as the reform of the European regulatory framework (the Regulation and the Directive for the Police and Criminal Justice Sector), surveillance activities and the right to be forgotten.

In response to recent developments in Europe, the WP29 also expressed opinions on a number of sector-specific and cross-cutting topics.

Through its opinions and statements, the WP29 is constructing an effective European data protection regulation.

Police and criminal justice aspects

Following the attacks in Paris on 7 and 8 January 2015, the WP29 expressed its views on the **European Passenger Name Record (PNR) system**. It recalled that, while it was legitimate to bring in measures to counter terrorist activities and the preparation of terrorist activities, these measures must be implemented in accordance with fundamental rights and respect for privacy and data protection. The European PNR system must obey the principles of necessity and proportionality.

The WP29 continued its analysis of the PNR agreements on transfers of the data of European passengers travelling to third countries, and in particular the United States and Mexico. It highlighted the lack of any legal basis for transferring European passengers' PNR data to the Mexican authorities.

It also examined the scenarios submitted by the Council of Europe's Cybercrime Convention Committee concerning direct cross-border access by law enforcement authorities to data stored in other jurisdictions.

Technology aspects

The WP29 produced an opinion on drones, and a code of conduct on cloud computing. It also pursued its analysis of the privacy policies of certain Internet majors (e.g. Google, Facebook, etc.), and its work on technical standards (e.g. ISO, Do Not Track).

Financial aspects and public sector aspects

The WP29 adopted guidelines on the automatic exchange of tax information, as developed by the OECD's Common Reporting Standard (CRS), and pursued its work on OECD standards in financial matters. It also analysed the European regulation on electronic identification, and the issue of publishing official representatives' data.

Cross-cutting topics

Following the CJEU's Google Spain judgement on delisting in 2014, which concluded that an Internet search engine operator is a data processing manager and subject to European law if one of its entities in Europe is involved in processing personal data, for example for advertising, the WP29 updated its 2010 opinion on the applicable law. It also worked as coordinator to handle complaints about the right to be forgotten.

Lastly, to achieve greater coherence in its work on cross-cutting subjects, **a new working group** was set up to be **in charge of cooperation aspects**. The group works on developing common cooperation tools (e.g. standard complaint form, organisation of workshops on specific topics, enhancement of the WP29 website, etc.) and aspects related to international cooperation (Global Prosecutors E-Crime Network, Spring Conference, International Conference).

INFO +

In 2015, the WP29 adopted 41 documents, ran eight working groups and held six plenary meetings attended by the European Union's 29 data protection authorities.

INTERNATIONAL AND EUROPEAN COOPERATION

Technological advances and globalisation firmly anchor issues of information technology and freedoms on the international scene. For this reason, the question of international and European cooperation seems to be a particularly strategic subject that is steadily gaining ground and requires an involvement in all of the initiatives that are developing.

This cooperation takes place within a number of forums, including the International Conference and the Spring Conference, as well as in more targeted forums such as the French-speaking association of data protection authorities (AFAPDP).

The 37th International Conference

In 2015, the 37th International Data Protection and Privacy Commissioners Conference was held in Amsterdam in the Netherlands and was attended by over 100 authorities and commissioners. During the closed session, two topics were debated: *genetic data and the supervision of surveillance activities.*

What challenges does genetic data pose for the future? (See full report in Part 1 on genetic data)

Given that a wide range of scientific, medical and personal information about individuals can be obtained from their genetic data throughout their lifetime, the authorities and data protection and privacy commissioners decided to conduct a number of joint observations into the way this data should be processed. It appeared especially important to state that the people concerned must remain in control of their data, receive appropriate information and see their decisions respected. This can be achieved through various resources that perform dynamic consent management throughout the data lifecycle. There are also additional safeguards, such as personal protection committees (CPP), privacy management programmes, privacy impact assessments, privacy by design, and certifications.

There have also been calls for the scientific community and the data protection and privacy community to work more closely together. This would allow the communities to develop a deeper mutual understanding and ensure that innovation continues to enjoy the benefits of genetic data while still guaranteeing that fundamental rights and consumer rights are upheld.

Supervision of surveillance activities, what is the role of data protection authorities in a society in the grip of change?

The amount of public debate on intelligence activities worldwide, along with changes in the security landscape as a result of the potential for terrorist activities in every country, have raised difficult questions for data protection authorities. The latter have identified several points on which their action would be important: the promotion of the principles of proportionality and lawfulness in intelligence activities; coordination with national and international surveillance bodies; the promotion of greater openness; the promotion of more extensive use of encryption as a legitimate means of protecting consumption data.

The next International Data Protection and Privacy Commissioners Conference will be held in autumn 2016 in Morocco.

AFAPDP, the French-speaking association of data protection authorities

In 2015, 48 of the world's 80 French-speaking countries had both a law and an authority to deal with data protection. There is still room for improvement in the protection of personal data in many countries. The latter can draw inspiration from the national texts and practices adopted by the countries represented on the AFAPDP, and the regional texts in force in Africa and Europe. The AFAPDP is pleased to see the cooperation established with the data protection authorities recently set up in Côte d'Ivoire, Kosovo and Mali.

The members of the AFAPDP, including the CNIL, adopted two resolutions at their general meeting in 2015. The first of these, inspired by the Canadian and European declarations, sets out fundamental principles to prevent any risk of mass surveillance and oversee the activities of the national intelligence services. The second resolution advocates taking ethical principles into account in the processing of health and genetic data. These two resolutions consolidate the foundations of a set of French-language data protection principles. The members of the AFAPDP also placed a resolution on data protection in the field of international humanitarian action on the agenda of the next International Data Protection and Privacy Commissioners Conference. The AFAPDP is also pursuing its work on pooling methods for overseeing application of the laws, begun in autumn 2015.

Alongside the coordination of its member network, the AFAPDP is open to various partnerships or cooperative initiatives in the field of fundamental rights. For instance, over the past year it worked with the network of French-speaking mediators and ombudsmen to educate children about their rights. ■

INFO +

The International Data Protection and Privacy Commissioners Conference

Since 1979, data protection and privacy authorities and commissioners from every continent have gathered to discuss the major emerging privacy challenges, in an international context marked by radical changes in technology, politics, the legal system and economics. The International Data Protection and Privacy Commissioners Conference consists of a closed session for all authorities and commissioners, and a session that is open to civil society and business.

3

TOPICS OF REFLECTION IN 2016

Data brokers: the oil and the iceberg

Connected vehicles: en route to the compliance package

From connected devices to autonomous devices: what freedoms subsist in a robotised world?

Data brokers: the oil and the iceberg

Data brokers are not a clearly identified legal category, but, given the importance they are gaining, they are attracting the CNIL's attention. By brokers, we generally mean professionals operating on a secondary data market. This definition covers several business lines that all tend to facilitate the circulation and enrichment of data.

THE OIL

For some years now, data has been seen as "the crude oil of the digital industry", powering the new economy's engine. And yet, the data trade is not held in consistently high regard and opinions vary widely on its subject. This contradiction is clearly seen in the opposition between those who believe in ownership of data and those who see data as the medium of a personal right. In its 2014 annual study, the Conseil d'Etat highlighted this opposition to discard the notion of "ownership" and consolidate the European approach by recommending the adoption of a right and a freedom, recognised in Germany by the Constitutional Court. This **right to informational self-determination** can be translated as the right of any person to decide on and control the uses to which their personal data is put. This right, which is written into the draft text on the Digital Republic, rejects the ownership aspect of the right to data.

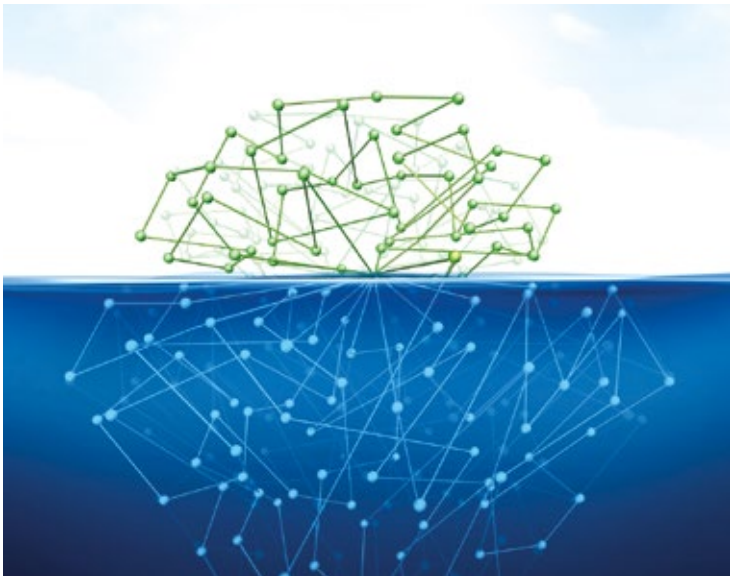
For example, the broker might act as a go-between for data owners keen to buy or sell data bases. Alternatively, the broker might act as a concentrator, aggregating and enriching data from partners, customers or public records on behalf of customers or on his or own behalf. In this last case, analysing the data allows the broker to offer value-added services (compilation, refinement of the profile and customer segmentation) to companies seeking to more effectively target their product and service offerings.

Though data brokering is still a little-known business in Europe, it is now clearly identified in North America, where **it is raising questions about transparency and about the degree of control individuals have over their data and its security.**

While the courts have recognised the commercial value of data files and the business of trading in files (see the Cour de cassation jurisprudence and more specifically its judgement of 25 June 2013), it is subject to its legality and without disregarding the rights of the individuals concerned by the data sold.

The issue at stake in data brokering is therefore the legality of the processing, which is ascertained by examining the characteristics of the processing carried out on the data in terms of the legal basis, purpose, proportionality and respect for the rights of the individuals concerned, apart from the type of formality applicable.

The French Data Protection Act unquestionably allows data to be circulated between recipients, and the emergence of new processing managers, themselves subject to a cascade of specific or common obligations, along with the initial data processor. The regulation on personal data protection also contains provisions that concern brokers, mainly because data brokerage aims, to a large extent, to allow the creation of profiles designed to automate actions.



THE ICEBERG

The existing legal framework, however, does not reflect the reality of data brokerage, because this data hub has the same features as an iceberg; the part we can see is only a very small fraction of the whole. Data brokerage aims to aggregate data then redistribute it for a variety of purposes, but which, for the moment, are focused on commercial targeting (direct marketing, advertising, customer experience enhancement), checking people's characteristics (trustworthiness, creditworthiness, identity) and combating fraud. In practice, the data is collected from a variety of sources, including international sources, which can range from open-source data to transfers of data collected by third-party data managers.

In marketing, the model entails aggregating databases built up for customer relations in retail outlets, with data from browsing, online orders or the use of information society services. The key for piecing all the different items of data together - whether they are named data, cookies, e-mail addresses, postal addresses or any other sort of data - is therefore essential for creating the profile.

The comparison to the iceberg lies at once in the way the profiles were produced (by gradually building up layers of scattered, but connected, data; then by consolidating data to form a coherent whole), but also in the invisible nature of the whole thus formed.

The question lies in the necessary transparency and the power that each person has to control the destiny of the data collected when they buy something in a supermarket, which is then used by an online brand to send an advertisement to a mobile phone.

Data brokers, though still relatively invisible, are one of the topics of reflection in 2016. ■

Connected vehicles: en route to the compliance package

Connected vehicles are a major strategic goal for car manufacturers, but they are also seen by many other professionals as a new opportunity to collect information or form a business relationship with motorists through new, more personalised and more relevant services.

On 7 January 2015, the CNIL organised the first gathering of the entire French connected-vehicle ecosystem. This initiative, carried out in partnership with the leaders of the *"big data"* plan in the *"New Industrial France"* programme, provided an opportunity to gauge the diversity of expectations and confirm the necessity of providing a framework for regulating personal data, based on the inclusion of privacy factors right from the product design stage (known as *"privacy by design"*).

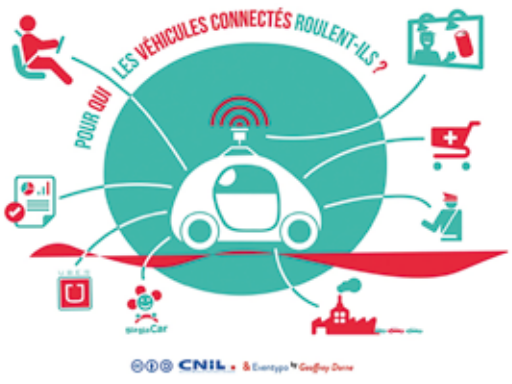
Alongside this approach, work began on a case study of the connected vehicle, to check whether the scenario-based approach was the right fit, since it had been used in earlier work on smart meters (or smart grids) and the use of energy data in homes. Throughout 2015, the CNIL consolidated its expertise in related subjects, such as electric vehicles, urban mobility, accident analysis and pay-how-you-drive systems, in order to give participants working on the compliance package a range of full studies.

THE KEY QUESTIONS ON INFORMATION TECHNOLOGY AND FREEDOMS

The first discussions with vehicle manufacturers, equipment manufacturers, insurers, start-ups and the police brought out two particularly fundamental questions for connected vehicles, which will serve as a common theme underpinning work on the compliance package.

The first of these obviously has to do with safety. Unlike "traditional" connected devices, the car is, by definition, moving in public areas. There is no need to remind readers of the road safety statistics: this "device" is not like the others, and safety is necessarily a key issue. The issue of safety and the confidentiality of personal data goes hand-in-hand, in this case of the connected car, with a cybersecurity aspect. The risk cannot be reduced to that of a breach of privacy, because interference with the driving information can have major if not vital consequences for the vehicle occupants and third parties.

The second issue concerns access to the data generated by the vehicle or its user. Evidence shows that the data generated in the vehicle will be a major issue. This data, whether it is technical, environmental or behavioural, is a substantial source of information for anyone who, for one reason or another, is associated with the car and its driver. Whether for vehicle maintenance, the marketing of vehicle-related goods and services, or smart cities, the connected car is set to become a key data platform.



A MOBILE PLATFORM

The recent adoption of the European regulation on the protection of personal data is, for many, a step towards the achievement of cooperation among authorities in Europe. Connected vehicles are, by definition, mobile throughout the European Union. To tap the full potential of this innovation, there needs to be harmonised European processing. Regarding personal data, the French and German authorities are now liaising to coordinate national research with a view to publishing the national results across Europe. The work on the compliance package will factor in the regulation scheduled for application in 2018, and so anticipate new rights such as the right to data portability or the privacy-by-design requirement.

> The work on the compliance package will factor in the regulation scheduled for application in 2018.

A QUESTION OF METHOD

Connected vehicles call for a partnership approach to address the industrial and innovation *issues* and the need to protect the freedom to come and go, without leaving anyone by the roadside. For this reason, the CNIL suggested that the compliance package should not be confined to a handful of stakeholders but opened up to the entire connected vehicle ecosystem in order to reflect the expectations, needs and requirements for protection. The stakeholders have been in talks since the end of February 2016 with a view to presenting their initial views at the Paris Motor Show in autumn 2016. ■

From connected devices to autonomous devices: what freedoms subsist in a robotised world?

Are we finally about to see a future with robots? For decades, science fiction has been predicting omnipresent robots. And yet, there does not appear to be any sign of them yet in our everyday life. But is that really the case? From industrial robots to "software robots", there are a growing number of signals... and of ethics and legal issues. The CNIL has decided to include this topic in its programme of study, to fuel a future-planning exploration of the ethical and legal issues entailed in robotics, through an economic and societal analysis.

Projections about the future size of the markets concerned are subject to caution, but experts agree that robotics will develop outside the industrial domain and evolve towards services in a wide variety of forms. In a 2015 report, the Institut Xerfi predicted opportunities in around 2020 for companion robots, drones, medical robots, robots to transport freight and passengers, etc.

The challenges in privacy terms are enormous. Companion robots will be used in the intimacy of people's homes, and medical robots are already being used in an environment that is inherently sensitive. In security-related domains such as transport and logistics, surveillance issues will be inevitable. Lastly, the use of robots in retailing, though admittedly still in its infancy, opens up new possibilities for marketing, CRM, targeting and monitoring.

ROBOTS: CONNECTED DEVICES LIKE ANY OTHERS?

The ingredients for a robot: sensors, computation and the means to take action

Connected or communicating objects are everywhere: smartphones, connected devices for the home (thermostats, bathroom scales, vacuum cleaners), devices that measure body constants (wristbands, watches), drones, cars, and more. They all have one thing in common, though: they make everyday objects "smart". But what exactly does "smart" mean? Put simply, it implies the addition of three capabilities: sensors, computational power and network communications.

Constant data capture in our everyday environment is a real novelty. This intensity of data capture digs a chasm between now and the world of traditional files, as we saw in the CNIL's second IP Report "The body, new connected object". Quite apart from the sensitive information found, for example, in medical records, we can capture seemingly

> A robot is a machine that has all the capabilities required to perceive, make decisions, take action and interact appropriately with its environment and the tasks for which it was designed.

insignificant data over long distances (number of steps, CO2 in a room, weight chart, sleep cycle, even location). As data accumulates, it becomes sensitive because we can deduce information about the individual, such as a statistical prediction of the person's future state of health.

Sensors are connected and then become communicating, either directly (over dedicated networks such as Sigfor or Lora) or via a smartphone, which has become the true connected device control centre.

The next step in this digital transformation seems to be to "make technology disappear", as explains Rand Hindi, from the French artificial intelligence start-up Snips, because constant calls are distractions that individuals would rather not put up with. So technology has to add the capacity to make decisions and act automatically, thanks to *machine learning*, *big data* or artificial intelligence.

As it happens, all of these features rolled into one form a robot, i.e. a machine that has all the capabilities required to perceive, make decisions, take action and interact appropriately with its environment and the tasks for which it was designed. Robotics is therefore a horizon for the Internet of Things.

The more "autonomous" a machine is, the more dependent it is... on data

By comparison with traditional connected devices, robots have greater autonomy. Autonomy implies the capacity to cooperate with humans in a common space: robots are becoming *cobots* (collaborative robots) that can act with humans and not instead of them or far away from them.

To do so, they have to collect far more data, which pinpoints a fundamental ethical paradox in the data protection domain: to be more autonomous, a machine must in fact become more dependent on personal data For example, an autonomous car must constantly capture what is happening around it [see box]. The same holds for an autonomous drone [see box]. In order to help isolated, dependent people, a companion robot has to collect data about the home, if only to avoid hurting the person it is supposed to help. It must also recognise the people present, which ▸▸▸

FOCUS

Drones: already almost flying robots

Drone regularly make media headlines. And yet, radio-controlled aero models have existed for a long time, even if they used to be difficult to control and were a pastime for real enthusiasts. Today drones look like flying smartphones and are easy to master, since they already have assisted flight capabilities. Recent models can take off, stabilise and avoid obstacles unassisted (thanks to their sense and avoid function). Others will even be able to automatically follow a person, for example to film them during a session on a bike or skis (in follow me mode). These technical feats rely on ever-growing numbers of sensors and volumes of data, especially concerning the user and the people nearby. Soon, drones will really be robots, carrying out tasks, sometimes even in a swarm, under more or less direct human supervision.

▸▸▸ may mean using biometric technologies such as face or voice recognition.

It is essential therefore to take an overall view of data governance and make privacy by design (which factors in privacy protection right from the design stage) a must for robotics. In a report entitled "Éthique de la recherche en robotique" (Ethics in robotics research), the CERNA (which studies ethics in digital scientific and technological research) (Allistène, 2014), has this to say: "While there is no way of stepping in at the design stage of a robot to prevent it from subsequently making an inappropriate or illegal use of the data it captures, the researcher should nevertheless make sure that the robotics system provides easy control of data usage."

INFO +

Autonomous cars: robots on our roads

The trend these days is towards developing partially or totally autonomous vehicles on the roads. The autonomous concept cars being tested have more and more sensors onboard, such as radars or lidars (for laser guidance). Some figures on the data collected suggest almost one gigabyte of data per second.

Given the particularly complex nature of road traffic, the autonomous aspect of these vehicles means that they have to be networked and able to learn collectively (for example, to cope with new situations). This is the road taken by some electric vehicle manufacturers, who exchange data in real time.

TOWARDS AN ETHICAL CONSIDERATION OF DIGITAL TECHNOLOGY AND A CULTURE OF DATA

Three ethical issues[1]

stand out in the robotics domain, each of them echoing data-related concerns.

1 | Repairing and enhancing the human body with machines

The ethical issues involved in using robotics on the human body are fundamental. Any use of technology on the body will create an imperative ethical need for respect for individuals' dignity, their right to informational self-determination and their right to choose freely without risking discrimination.

2 | The imitation of life, and affective and social interactions: towards true man-machine interactions that respect individuals' rights?

How far can we trust robots? How can we account for their behaviour? "We will have to rethink consent in a robotics environment, especially as the risks of emotional manipulation of the person are high", pointed out psychologist Serge Tisseron during the hearings before the Office Parlementaire d'Evaluation des Choix Scientifiques et Technologiques in December 2015[2]. Robots enable sophisticated man-machine interactions; they must also enable a context-sensitive, explicit dialogue that is tailored to the person's wishes.

3 | Autonomy and decision-making capabilities: up to what point should technology be making decisions for us?

Lastly, robotics poses a general ethics question concerning the user's ability to take action. For the CNIL, it is not always necessary to make a distinction between a mechanical robot and a software robot in order to consider the regulation of decision-making autonomy. The question of the transparency of algorithms, or at least of their rules, and the transparency of the ability to understand how decisions that affect people are made by autonomous systems, are fundamental ethical questions for future. ■

1 The CERNA report mentioned earlier gives the details of these issues.
2 OPECST, "Les robots et la Loi" (Robots and the law), public hearings on 10 December 2015.

Commission nationale de l'informatique et des libertés
8, rue Vivienne
75083 Paris Cedex 02
Tél. 01 53 73 22 22
Fax 01 53 73 22 00

www.cnil.fr

Conception & réalisation graphique
LINÉAL 03 20 41 40 76 / www.lineal.fr
Crédit photo CNIL, Fotolia, istockphoto

CNIL
Commission Nationale de l'Informatique et des Libertés