INNOVATION, ENTREPRENEURSHIP, MANAGEMENT SERIES

INNOVATION AND TECHNOLOGY SET

Volume 1

Security and Privacy in the Digital Era

Claudine Guerrier

ISTE

WILEY

Security and Privacy in the Digital Era

Innovation and Technology Set

coordinated by
Chantal Ammi

Volume 1

Security and Privacy in the Digital Era

Claudine Guerrier

ISTE

WILEY

First published 2016 in Great Britain and the United States by ISTE Ltd and John Wiley & Sons, Inc.

ISTE Ltd
27-37 St George's Road
London SW19 4EU
UK

www.iste.co.uk

John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030
USA

www.wiley.com

Library of Congress Control Number: 2016943714

British Library Cataloguing-in-Publication Data
A CIP record for this book is available from the British Library
ISBN 978-1-78630-078-2

Contents

Introduction

"If Marx were to return, which phenomenon would he use to characterize today's society? It would no longer be capital or capitalism, but rather the development of technique, the phenomenon of technical growth"[1]. Control technology revolves around the assessment of techniques and tools, and its importance became apparent as early as the 19th Century. The relevant literature flourished between the 1930s and the 1980s. One name that stands out in particular is Jacques Ellul, Professor of Law at the University of Bordeaux, especially known as a legal historian and a sociologist. As a commentator on the rise of capitalism and a personalist, Jacques Ellul considers the technical tool as being at the heart of society. Ellul's "technician system" [ELL 12] puts alienation at the center of technicist capitalism. For Ellul, tools and machines are singled out. They play an essential role in the economy and the fabric of society. The influence of Ellul's ideas has gone beyond French borders and has reached the United States. The importance of machines has been recognized for a long time, with the growth of the working class and the *bourgeoisie*. It follows the rise of services and innovation. It can be seen in inventions and intellectual property law; with its international conventions[2], strategic analyses that commercial societies carry out to determine whether certain patents should have a limited reach, within one or several states, or whether they should reach a number of countries. Machines are often mobile: from 1980 onward

1 Jacques Ellul, interview with Jean-Claude Gillebaud, Le Nouvel Observateur, 17 July 1982.
2 Convention de l'Union de Paris, PCT Convention, Munich Convention.

and especially from the start of the 21st Century they are nearly always mobile, participating in a level of control that the users are not always aware of, or to which they are consciously indifferent. This is what appears in the "profiling of populations" [MAT 14], which breaks down and analyzes the outlines and dynamics of post-Orwellian surveillance, and sometimes even cyber surveillance.

For several decades now we have been living in the digital age. Digitization is relevant to nearly all tools and machines. Development must occur digitally. In the domain of electronic communication, where audiovisual technology is joined to telecommunications and informatics, digital technology prevails. In France, the 2016 law on digital technology was one of the most important legal contributions provided by the Valls government, and came after consultation of the various parties involved. Very high speed broadband is an objective for both states and companies. Many nations of Eastern Europe, including those previously belonging to COMECON, have successfully focused on the growth of fiber optics to compensate for their bad start with the triumph of the copper pair in Western Europe. Lithuania was ranked first among European countries in terms of the penetration of fiber optics in its plastic form or as a glass fiber, while the United Kingdom and Germany, where the copper pair had previously allowed for the installation of comprehensive networks, were placed outside of the rankings. This is also the case in Estonia, Poland and Russia (not in the European Union), and even Belarus. The European Union has established a plan for the growth of very high speed broadband that is to be finalized in 2020, which seems optimistic. European funds were made available, but have since been reduced as a result of the levels of debt that are affecting nearly all European states. The governmental public subsidies are more readily approved by the Commission when the country in question belongs to the old Soviet block, which converted to a market economy only 25 years ago, than when the country has belonged to the liberal sphere for much longer. With regard to mobile phones, while research on 5G has progressed considerably, most private telecommunication operating companies in the developed world use 4G licenses. Digital technologies are a prominent factor for growth, but the digital divide is still a reality in Africa, despite being presented as a continent that is favored for development. With regard to fiber optics, this divide is obvious between

highly urbanized areas and medium-density or low-density areas. The question is whether territorial collectivities can play an active role in the complex situation. In France, since LCEN[3], territorial collectivities are not only able to develop networks – which they have been able to do since 1999 because of the general code of local collectivities – but can also be network operators. Also in France, local collectivities have been granted WIMAX licenses. However, the same choice has not been given in all countries of the European Union, which, as part of a neo-liberal agenda, encourage an informed distrust of public collectivities – if they are regions – participating in the exploitation of networks, or even of communication services. The Treaty on the Functioning of the European Union, following previous treaties that constitute it, allows for a reasoned and argued amount of leeway in terms of services of general interest, which could be technical or economic exceptions, not only for digital technologies, but also other technologies that are likely to boost the market and competition.

Digital technologies are a dominant factor among those that shape us and that we govern (unless it is these technologies that govern us). Nanotechnology is a technology that affects the state of the environment, whether these be techniques that use renewable energy or technology that deals with the various forms of the ecosystem, plant, mineral or animal matter, join together digitally to substantiate commercial exchanges between long industrialized countries or those only recently so, between emerging countries – not only Brazil, Russia, India, China and South Africa (BRICS), but also Indonesia, South Korea, Mexico, Turkey, Saudi Arabia, members of the G20, between developing or even underdeveloped countries, but with investment zones that allow for interesting and worthwhile returns on investment. The techniques, often coupled with services, are therefore at the heart of the system – as described by Ellul – which has an economic dimension, but also a legal dimension, with a strong focus on legal rationalization, and a geopolitical dimension, since technicist systems also involve a military dimension, with satellites and drones that draw upon a civil and commercial aspect as well as a military one, linked to a military

3 Law for trust in the digital economy of June 21 2004, which transposes the directive of June 8 2000 on electronic commerce, and also covers cryptology, essential in electronic commerce, and territorial collectivities in the sector of electronic communication.

industrial complex, not only in the United States, and to alliances where the United States continues to play a determinant and predeterminant role in the context of NATO, but also with states that are not members of the North Atlantic Treaty Organization (NATO), but which rely on the help of NATO on multidimensional issues that pit them against other entities, states, international organizations, lobbies and various diverse companies.

The techniques and technologies mentioned above can be exploited with the goal of commercial benefits, but they can also be used for the upkeep of national security and public order. They have a lot of potential in terms of surveillance and control. As such, with regard to secret correspondence, postal letters could be opened and read, in the French "Cabinets Noirs" in the 19th Century, for example. In "Lucien Leuwen" by Stendhal, the interception of a telegraph results in the winning of an election. At the end of the 20th Century, a landline telephone could be listened on legally in certain cases. With the popularization of personal computers and mobile telephones, it has become much easier for citizens to communicate among themselves; it is also much easier for the State to intercept various methods of communication through conversations, e-mails, text messages, etc. The materials used are cheaper, as are the methods of interception. At the end of the 20th Century, operators carrying out interceptions legally have often come up against the Ministry of the Interior and the Ministry of Justice, as these interceptions, which constituted a public service, were deemed underfunded in the eyes of those with a background in private law, as much in the United States as in other developed countries. Public authorities, attempting to protect taxpayers' money and the government coffers, found themselves in contradictory positions, and negotiations were long and difficult. In the 21st Century, the price of an interception is much lower and as such the number of interceptions is always increasing. The search for profit is identical for commercial societies, but the context is less rigid, and negotiations between operators working for the State and the State itself are less difficult. The interception of electronic communications is a field that has progressed, but the methods of interception have existed for a long time.

Other forms of technology have, like interceptions, boomed in the 21st Century, while having contributed to the upkeep of public order in the 20th Century, or even in the 19th Century. Robotization and the replacement

of a human workforce by intelligent machines fit into this logic. However, other surveillance and control mechanisms have appeared during the 21st Century and can be added to those already in place. Among those technologies that existed previously but which have grown exponentially during the 21st Century, biometrics and CCTV are two of the most prominent examples.

Biometrics was first of all anthropometrics[4]. Fingerprints were used during the course of the 19th Century. During the 20th Century, a distinction was made between morphological biometrics and behavioral biometrics, which would not have been relevant to anthropometrics. Moreover, the rate of false negatives and false positives appeared in the 20th Century as a way of measuring the reliability of a biometric method[5]. Among these methods, fingerprints, iris recognition and retinal scanning are all very reliable. Fingerprints are currently the method most used by the State faced with an increasing demand for free circulation since the unification of passports and visas at the level of the European Union; fingerprints are also used in airports for access to reserved zones, and for sensitive routes, such as those headed toward Tel-Aviv. Iris recognition was the object of a patent in the United States, but this patent is currently in the public domain, even though iris recognition is more often used in the United States than in Europe, for reasons of intellectual property, but also for cultural reasons. The irises of monozygotic twins are different and the rate of false negatives/positives is infinitely low. Furthermore, access to the iris is not problematic with regard to the individuals concerned. Retinal scanning is as reliable as iris recognition, but requires the assistance of an ophthalmologist, and thus is limited to prison services. Palmar recognition results in a three-dimensional (3D) image of the palm of the hand and is quite reliable, but less so than fingerprints or ocular techniques. However, it is quite popular in most developed countries as it can restrict access to canteens reserved for adults, adolescents or children, and help with adherence to working hours within companies[6]. Facial recognition is less reliable, and is used more in the

4 See Berthillon.

5 The rate of false negatives corresponds to a biometric method calling a negative when it should have been accepted; the rate of false positives corresponds to passes that should have been rejected.

6 Palmar recognition is preferable for an employer over a badge, which can be used by someone else other the employee or the collaborator intended to use it.

United States than in Europe. However, mistakes between delinquents and presumed delinquents later shown to be innocent in the United States have shown that this method is less reliable than fingerprinting. Facial recognition has been most popular in the United States during large meetings. In the United States and in most European countries, facial recognition is coupled with CCTV during sporting events. Behavioral biometrics is usually considered to be less reliable than morphological biometrics. There are a variety of behavioral biometric techniques, such as vocal recognition, typing patterns, biometric signature and shadows. Vocal recognition was the subject of a famous literary illustration in "In the first circle" by Solzhenitsyn [SOL 09]. The first circle is that of the zeks, intellectual researcher prisoners, whose knowledge and creative imagination could be massively useful for the Stalin regime. In this work, there is much reference to one prisoner's research on vocal recognition. The prisoner is passionate about his work, but also conscious of its limitations. The regime is looking to use the system created by the zek, but in the 1950s the rate of false negatives/positives was high and it would inevitably result in the imprisonment of "innocents" alongside the sought-after "enemies of the people". Vocal recognition has come along greatly since "In the first circle". Various programs have been able to improve the performance of most of the existing methods. However, vocal recognition, even when improved by computer programs, is not very reliable. The same is true for nearly all behavioral biometric techniques. Biometric signatures are not accepted by the CNUDCI[7]; it is rarely used in legal proceedings. In the United States, the State of California recognizes it and allows it to be used, but Californian individuals and professionals are far more likely to use an electronic signature over a biometric one. Genetic profiling can be included as a morphological biometric, but other distinctions place it in a separate category. Contrary to popular belief, a genetic profile is not 100% reliable. However, it is without a doubt the most reliable. This being said, it is highly invasive with regard to personal and collective freedoms, and as such it is only used and centralized following very precise and detailed rules that cannot be breached. Files containing genetic profiles are problematic in terms of protecting personal data; this must be kept in mind for the future.

7 United Nations Commission on International Trade Law, initially model laws that served as references for arbitration, for bank guarantees, for legal questions inherent to electronic commerce.

During the 21st century, much research has been carried out on biometric applications. Businesses gladly finance this research as the new methods are quickly used and provide a generous return on investment. This is why progress has been made for all the existing processes, and also why many possible new paths have been explored: venous system, earlobe and outline of the lips are just a few examples. Biometric processes become part of social life and allow for collective (passports, visas) or individual (adherence to work hours) methods of control. The main actors are States, commercial societies, and international organizations are also keen to be part of the biometric game[8].

CCTV has been around for a long time, but has only become widespread in the past two decades. It appeared in Nazi Germany, which often drew upon the military[9] and civilian aspects of science in order to achieve its goal of world domination. However, CCTV really rose to prominence after the Second World War. The first country to embrace it fully was the United Kingdom, starting in the 1950s, where it went through a boom in the 1990s. Currently, cameras (analog, and now digital too) are in place all over the United Kingdom, from motorways to public transport, shops, etc. This systematic placement of cameras has allowed British researchers to gain some insight into the installation and maintenance of such methods of systematic surveillance. It would seem that levels of delinquency and criminality are not affected by this generalization of CCTV, and yet British security ideologies draw on the need to fight them, as well as terrorism after the attacks of July 7, 2005, to justify public spending in this domain. CCTV has certain areas of brilliance: the road network – the end goal is to the combat highway code violations and reduce accidents, reduce mortality and disability; public transport – the objective is to protect travelers against various forms of delinquency; shopping centers, banks – the objective is to reduce theft; establishments open to the public, such as hospitals and universities – the objective is to guarantee the safety of users and visitors, patients, students, etc. In the United Kingdom, this is financed either publically or privately.

CCTV has spread to most developed countries and even to some developing countries. It has gained popularity most notably in the United

8 UNHCR, particularly in Afghanistan.
9 Attempt to obtain the atom bomb, significant competitive advantage.

States, but less quickly than in the United Kingdom. In France, CCTV was only used patchily up until the end of the 20th Century; the first important law regulating it is from January 21, 1995. This law, which remains an essential one, states that the film produced is of a personal nature, and must give rise to a declaration. The rise of CCTV in France is first of all the result of town councils and their councilors. In France, the installation of CCTV cameras must follow a request made to the prefect, who collaborates on this matter alongside departmental commissions. In Paris, the authorization request is submitted to the prefect of the police of the City of Paris. The aims are similar to those in the United Kingdom, and involve the safety of individuals and of their goods. The following are the main areas involved: sides of buildings that can present a risk, road traffic to prevent violations and accidents[10], national Defense buildings, public transport – particularly the metro and the bus – and shopping centers. CCTV is also mainly focused around establishments open to the public. In France, all authorization requests must involve the submission of a file to the prefecture, with an overall and individual plan for the placement of each camera. The individuals involved have a right of access to any film involving them, as this corresponds to personal data via image identification. After use, the film is destroyed, except if they constitute evidence to be presented in front of a court or tribunal.

Funding in France was first rather limited, as many prefects and mayors saw little use in the installation of cameras. It was therefore political volition that led to the increasingly widespread installation of CCTV cameras. In France, an installation plan was drawn up by various successive interior ministers, and the accompanying legislation was LOPPSI 1, followed by LOPPSI 2.

In all nation states, politicians have relied on a latent feeling of lack of safety in most citizens, exploited during the broadcasting of various current affairs: crimes and especially petty delinquency. Citizens have the largely fallacious belief that they are protected by the presence of cameras, which supposedly would dissuade criminals and delinquents to commit a crime. This feeling is largely erroneous: at most criminals are led to carry out

10 However, there is no clear correlation between the decrease over the last 10 years of the number of deaths on the roads of France and the installation of security cameras.

their acts elsewhere, and even then this change is usually fleeting. In France, the terminology has been changed to further propagate this popular fear, largely exploited by the media and elected officials. Since the LOPPSI 2 law of March 14, 2011, the term used is no longer *videosurveillance* but rather *videoprotection*, which seems more correct and more positive.

However, seeing as videoprotection is a method of control in most countries contingencies are planned in the case of abuse. In France, a national commission for videoprotection has been set up. Subsequently, the CNIL has been given the general mission of protecting personal and collective freedoms as protected by the European Council's European Convention for the Protection of Human Rights and Fundamental Freedoms[11], which is the European charter of the fundamental rights of the European Union[12]. Complaints are submitted to the CNIL if the goal pursued by the recording is alleged to not be the safety of individuals or their goods. In nearly all industrialized countries, employees are filmed during their workday. The goal is to ensure the safety of goods, materials and collaborators; constant surveillance of the employees is incompatible with the reference texts on the matter of freedoms[13]. Even consent on behalf of the employees is incompatible with these texts. Consent does not make these types of operation legitimate. Neither the company nor the employer is within their rights to use the cameras for management to increase the efficiency of workers, or to increase competition in the company. However, it has become clear that misuses occur, and the number of complaints made to the relevant bodies has increased. In France, the CNIL receives these complaints. Formal notices made public are relatively rare, but the number of complaints is steadily increasing, suggesting that some people, despite the influence of security-driven ideologies, are not close to accepting being under surveillance during their entire working day.

While interceptions and videoprotection have existed for a long time and have become increasingly prominent in the social context of the 21st Century, some methods have only come into existence during the 21st Century: the body scanner and genetic profiling are the most notable examples.

11 Article 8 on private life.
12 Articles 7 and 8.
13 See CNIL report on cybersurveillance at work 2004.

According to Bruno Latour, "techniques are governed by means, and morals are governed by ends, even though, as declared by Jacques Ellul long ago, some techniques end up going beyond the world of ends by giving themselves their own laws, by becoming autonomous and no longer only automatic" [LAT 00]. Techniques have gone beyond the world of ends: this is the case for biometrics especially, a factor of digital identification.

The body scanner first appears to belong to the world of means, but the question of its relation to the world of ends remains unanswered. There are two types of body scanners: the millimeter wave scanner and the backscatter X-ray body scanners. The most often used is the millimeter wave scanner; this is the case in the United States, the United Kingdom, the Netherlands, Germany, Italy, France and Canada. Body scanners work using microwaves. The domestic appliances that use millimeter waves play an important role in western countries inside microwave ovens,[14] mobile telephones[15] and WiFi networks[16]. Only an insignificant amount of the radiofrequency energy emitted by the scanner is absorbed at the surface of the body, while most of the radiation is reflected and detected by sensors so as to produce a 3D image. The scanners are mainly used in airports, despite the principle of freedom of movement, which is part of economic law, freedom of commercial exchange and human rights[17].

Body scanners have been installed in large numbers in the United States: in 2010, 385 high-cost scanners had already been installed in more than 60 airports. The United States has also initiated the installation of body scanners in the airports of most western countries, with the goal of increasing the safety of air travel. Some countries are resisting this American pressure, but the United States's closest allies are following its example.

In the medical domain, studies have been carried out. They have not come to definitive conclusions, but do feed into fears of cancer. Should the principle of precaution be applied? In the United States, the answer is no.

14 24 to 30 GHz.
15 0, 9 to 2, 1 GHz.
16 2,45 GHz.
17 Article 2.1 of the International Covenant on Civil Rights, 1966, "Liberté d'aller et de venir".

Many Americans consider that the body scanner is an affront to privacy: the scanner reveals the intimacy of the individuals scanned, if only to the TSA agents scanning[18]. A high number of citizens are worried that their photographs might find their way onto the Internet, including social media. A boycott movement was started on the eve of Thanksgiving Day 2010. Thanksgiving was chosen as it is a day when Americans travel a lot, many using airports. The right to intimacy and privacy, which is purportedly violated by the body scanner, was relayed by numerous human rights groups. Consequently, Epic[19] lodged a complaint to suspend the use of body scanners in American airports for being "illegal, invasive and inefficient"[20]; this complaint has not come to anything. American authorities, in the context of ever-present geopolitics, are pressing European governments to reinforce security in air travel and to introduce body scanners.

At the level of the European Union, the European Parliament has asked, in a resolution on October 23, 2008, for a report to be carried out evaluating the effect of body scanners on health and in terms of fundamental rights. The Commission has been invited to consult the controller of European data protection, the EU Fundamental Rights Agency. A debate was organized in January 2010 by the Commission on Civil Liberties during a meeting with the coordinator of antiterrorist policies[21]. The policies regarding the installation of body scanners are meant to be included as part of a bigger movement of data sharing between the European Union and the United States. The deputies of the Commission on Civil Liberties are of the opinion that before body scanners are introduced, the Schengen information system and the visa system must first be evaluated to determine whether these systems are efficient and follow the principles that govern personal data protection. A debate next took place in front of the transport select committee in January 2010. Some ambivalence was apparent in terms of privacy. Certain individuals, such as the Britain Jacqueline Foster, were favorable to profiling and information exchange to increase the reliability of technology. Others, on the contrary, were above all attached to the preservation of privacy. This required that, at the least, the images be not

18 Transportation Security Administration.
19 Electronic Privacy Information Center.
20 Epic.org/ privacy/airtravel/backscatter.
21 At the time, Gilles De Kerkhove.

released to the press. Furthermore, it is vital that images, which are identifiers, be destroyed immediately after use. While airport controllers are currently not allowed to save the pictures created, it would only take the use of a mobile phone for a quick picture to be taken: any misconduct could lead to the copying of an image of an adult's or child's body onto a digital platform. On June 15, 2010, the European Commission presented a report on the body scanner. The goal of the scanner is to detect objects and not identify physical individuals. As a result, no image created by the scanner can be kept. If this is not the case, such as with the creation of passenger image files, the goal has been changed, violating directive 95/46 of the UN General Assembly resolution of December 14, 1990. Moreover, the person cannot be identified: as such the face must be blurred. Identification can only be made possible if dangerous objects are discovered. To ensure the anonymity of the individuals scanned, the controllers must work in pairs: one must help get the passenger into the scanner; the other looks at the visualization screen and carries out the control, but without direct contact with the passenger undergoing the control.

On May 24, 2011, the European Parliament Committee on Transport and Tourism voted for the report produced by the conservative Luis De Grandes Pascual[22] from Spain, with a very large majority. The report is focused on air safety and most importantly the use of body scanners in airports.

The use of body scanners is a factor for the consolidation of air safety. The machines were trialed in the United Kingdom, Netherlands, Finland, France and Italy[23]. Since 2008, when the European Parliament signaled its opposition to the introduction of body scanners, the situation has changed greatly: "four years later (…) we consider that these devices can provide added value in terms of safety, without any health risks for passengers or issues regarding their fundamental rights". The report asks member States to "use the available technology that is the least harmful[24] possible for the health of individuals" and to ban scanners that use ionizing radiation, meaning scanners using X-rays, out of consideration for more vulnerable

22 PPE.

23 In Italy, body scanners were deployed in several of the country's airports, but these were removed after several months as they were deemed useless and incompatible with privacy, as stated by Vito Riggio, president of ENAC, l'Ente Nazionale per l'Aviazione Civile.

24 The report does not claim to achieve absolute safety.

people. These include pregnant women, the elderly, children and sick people.

Privacy must be respected. Refusal to pass through the body scanner results in having to submit to another form of inspection, that is equally effective, such as a full body pat-down search. Refusal "must not be the cause of any suspicion toward the passenger". Luis De Grandes Pascual does however recognize that a pat-down search, as seen in the United States, can complicate and delay boarding for passengers refusing to pass through the body scanners. When individuals accept to pass through the millimeter wave body scanner, a random selection is made and the passengers cannot be chosen based on discriminatory criteria: "Any form of profiling based notably on gender, race, skin color, ethnicity or nationality, genetic characteristics, language, religion or beliefs is unacceptable". This is perfectly compatible with directive no. 95/46 and with the current regulation project. The image cannot be an absolute method of identification. Humanity dignity and intimacy must be considered. Only "stick-figure"[25] type outlines can be used. No images of human bodies can be saved or stored. According to the eurodeputies, the images are destroyed immediately after the security check has been carried out. Most importantly "the technique used must not allow for data preservation or recording".

Eurodeputy Sylvie Guillaume has stated on her blog that considerable progress has been made since 2008, and that various criticisms concerning health and private life have not been ignored. However, she remains skeptical with regard to the usefulness of millimeter wave body scanners. Other control techniques, that are supposedly less intrusive, are currently being trialed in airports. The body scanner has never been shown to be particularly effective. No convincing study has even proven its added value in terms of fighting terrorism – the principal argument behind its installation in the first place. German conservative Markus Ferber is more reserved on this than Sylvie Guillaume: "Body scanners intrude on the private sphere, without any clear gains in terms of safety". Sylvie Guillaume stresses the link between the technique and industry: several companies have placed body scanners on the market that are expensive but that are able to provide considerable return on investment for the manufacturers. The latter group

25 "*Bonhomme-allumette*".

constitutes an important lobby regarding control in airports and they know how to make their voices heard. They are able to modify their machines, their products, so as to make them compatible with the legal requirements regarding privacy and personal data.

Eurodeputies are asking for a form of collaboration to be set up at the level of the European Union in the domain of air safety. This would involve mutual recognition of the measures considered, as well as a single form of security control for all passengers, luggage and freight in the airports of the European Union. This is a form of coordination between the States of the European Union. Discussions are still taking place between the USA, initiators of the installation of the body scanner, and the European Union, which is undoubtedly more stringent than the United States in terms of health and the respect of privacy.

On July 6, 2011, the European Parliament passed a resolution to outline the use of body scanners, drawing from the Pascual report. The report predated the Commission's decision to authorize the use of body scanners in airports. The Parliament is within its rights to cancel this decision, within a period of 3 months. The European deputies asked that the European governments equip themselves with the relevant technology before the end of April 2013, which marked the end of the ban on transporting liquids through the air. This is why the Commission, wishing to enforce the deadline of 2013, announced the establishment of a working group comprising representatives of the different States and prominent members of the relevant industries and the aviation sector.

The Commission stated that passengers would not be chosen "only" based on criteria such as gender, race, skin color, social background, ethnicity, religion or beliefs[26]. However, this constitutes sensitive data, and directive 95/46 considers that the personal data of this category cannot be stored and used pre-emptively, except in cases where consent is given beforehand. Individuals chosen to be scanned by millimeter wave body scanner in this way are clearly being subjected to discrimination. There is a risk of profiling, whether racial or of another form. How often the word "only" will be applied must be determined.

26 Commission communication to the European Parliament relative to the use of security scanners in airports of the European Union, COM (2010) 311,§50.

The European Commission has decided that to "not risk compromising the health of citizens, only body scanners not using X-ray technology are allowed for the control of passengers in airports within the European Union. All other technology, such as that used in mobile telephones and others can be used as long as they adhere the European Union safety standards". This was met with negative reactions in the United Kingdom in two airports using X-ray scanners, Manchester and Heathrow. Manchester airport issued the following statement: "Thorough tests have been carried out by the UK Health Protection Agency and the American health authorities have already confirmed that body scanners present a negligible risk for human health. It is irresponsible to imply that, since Europe has not yet finished its health study, our passengers should be concerned. This week European legislation approved the use of millimeter wave technology, another form of body scanning technology, for permanent use in airports…Given that all competent authorities allow for the use of X-ray scanners, it shall continue to be used". At Heathrow, the situation is different. The airport had previously used X-ray scanners as part of a trial of the different body scanning technologies, but once the evaluation had ended the airport exclusively used millimeter wave body scanners. In France, Aéroports de Paris was lucky to have anticipated the correct choice, as experiments in Paris used the millimeter waver scanner. In France, it is the LOPPSI 2 law[27] that regulates body scanners. It follows recommendations made by the G29[28] and the CNIL.

The observation of images is limited to competent and experienced personnel within areas not open to the public. Those carrying out the control are of the same gender as the passenger. These arrangements had been previously introduced for pat-down searches. The preservation of images is limited to the amount of time necessary to carry out the test. Observation of the images is done in areas closed to the public and limited to the relevant staff. Most importantly, bag searches can only be carried out with consent from the person being controlled. If this is refused, the person can go through another form of control, usually a pat-down search, which causes problems itself with regard to intimacy and privacy. The body scanner

27 Law of March 14, 2011.
28 Meeting of the representatives of the regulatory authorities as part of directive 95/46, in reference to article 29 of the directive.

cannot be used without clear and informed consent. Analysis of the images observed is done by operators who do not know the identity of the individuals themselves and who are unable to observe the physical individual at the same time as their image produced by the body scanner.

Genetic files, which relate to biometrics, but which are used by the police, involve the use of effective technology that appeared and started to be exploited at the end of the 20th Century and at the start of the 21st Century.

Genetic "fingerprints" are assimilated to biometric data. Biometrics, according to the dictionary definition[29], is "the science that studies, using mathematics (statistics, probabilities), the biological variations within a determined group". This definition can be applied perfectly to DNA. Moreover, regulatory authorities, such as the CAI[30] in Quebec or the CNIL in France, also add the analysis of genetic fingerprints to the distinctions mentioned above between morphological biometrics and behavioral biometrics. British and French genetic files quickly raised issues with regard to the equilibrium between security, public order and the preservation of privacy.

On December 4, 2008, the Grand Chamber of the European Court of Human Rights found the United Kingdom guilty of violating article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[31].

Two British citizens, S[32] and Michael Marper[33], were at the origin of this affair.

The first claimant was arrested on January 19, 2001, and indicted with attempted theft with assault; he was 11 years old at the time, a minor. The police obtained his fingerprints and DNA samples. He was acquitted on June 14, 2001. The second claimant was arrested on March 13, 2001, and

29 Petit Robert, 2014.
30 Commission d'accès à l'information.
31 ECHR, December 4, 2008, numbers 30562/04 and 30566/04, Set Marper c/United Kingdom.
32 The first claimant.
33 The second claimant.

indicted with harassment of his partner. The police obtained his fingerprints and DNA sample. Michael Marper's partner later reconciled with him, and abandoned the charges: on June 14, 2001, the case was closed.

The claimants asked that their fingerprints and DNA samples be destroyed, and were denied by the police. They decided to take this to court. On March 22, 2002, the administrative tribunal[34] rejected their claim[35]. On September 12, 2002, the court of appeals confirmed the decision of the administrative tribunal with a majority of two votes to one. On July 22, 2004, the House of Lords also rejected the claim. The result was announced by Lord Steyn, in the name of the majority.

Having exhausted all internal routes, S and Marper submitted an individual request to the European Court of Human Rights (ECHR). Their claim was against the storage of their fingerprints, cell samples and genetic material. They focused on articles 8 and 14 of the European Convention on Human Rights and claimed that article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms regarding privacy had been violated. The court first looked at whether the preservation of fingerprints, cell samples and DNA profiles of the claimants could be considered a form of mismanagement of their private life. The ECHR judged that the general and undifferentiated character of the storage of fingerprints, biological samples and DNA profiles of individuals suspected of having committed a crime, but not convicted, does not constitute a "just balance" between the public and private interests: it was therefore a disproportionate violation of the rights of claimants, the respect of privacy and is unnecessary in a democratic society. Article 8 of the convention had indeed been violated, and there was no need to separately examine the claim regarding article 14 of the convention. The United Kingdom had to pay 42,000 euros to the claimants for fees and expenses.

The British government states that the risk of intervening in private life is limited by the law and the technological processes of extraction[36]. The ECHR mentions that a distinction has already been established between the

34 Lord Justice Rose and judge Leveson.
35 EWHC 478.
36 "An individual shall only be identified in the case of concordance of their profile with one of these elements and within the scope of this concordance".

preservation of fingerprints, cell samples and DNA profiles. The issue of respecting private life must be analyzed separately for the storing of cell samples, DNA profiles and fingerprints. Previously[37], the ECHR has judged that in the case of cell samples, systematic storage of these elements was too intrusive. "Moreover, the samples contain unique genetic code of great importance to the person concerned as well as their family". The court also mentions that the concept of a private life is a broad one. "…The simple act of storing data relative to the private life of an individual goes against article 8". An act of mismanagement is considered essential for achieving a legitimate goal in a democratic society if it is proportionate to the legitimate goal in question, and if the reasons stated by the national authorities seem to be "pertinent and sufficient"[38]. Some leeway is allowed for national authorities. However, fingerprints, DNA profiles and cell samples "all constitute personal data in the eyes of the Convention… as they relate to identified or identifiable individuals". The various forms of biometric data are analyzed, especially DNA profiles, which "provide a method for discovering genetic relations (and ethnic ones) that can exist between individuals, which is sufficient to conclude that their storage is itself a violation of the privacy of these individuals". A similar reasoning can be applied to digitized fingerprints. The ECHR recognizes that the fight against crime is a legitimate goal. Among the methods deployed in fighting crime, the Council of Europe has recognized that DNA analysis techniques present certain advantages. However, the question that arises is could the storage of fingerprints and DNA information belonging to S and Michael Marper, suspected of having committed crimes but not convicted, be justified under article 8 section 2 of the convention? The ECHR states the England, Wales and Northern Ireland are the "only jurisdictions with the Council of Europe that authorize unlimited storage of fingerprints and DNA profiles and samples of any person, regardless of age, suspected of having committed a crime registered with the police". Other States have decided to set limits for storage and the use of these data so as to reach a balance between public order and the maintenance of rights to privacy. The United Kingdom insists on the effectiveness of these data in the case of a crime being committed. Neither statistics nor the examples provided suggest that it would be impossible to identify or to chase those committing crimes without

37 Aff. Van der Velden, December 7, 2006.
38 CEDH, January 18 2001, no. 24876, Coster C/United Kingdom.

the permanent storage of fingerprints or DNA profiles. Moreover, the storage of information regarding individuals who have not been convicted is all the more worrying when they are minors. The ECHR has stressed the importance of preserving the privacy of minors during legal proceedings[39]. Within the United Kingdom itself, Nuffield Council expressed its reservations concerning the possible consequences for young people of having their samples and DNA profiles preserved for an unlimited amount of time: minors and members of minority ethnic groups not convicted of a crime are overrepresented in the database.

The ECHR judges that there has been a disproportionate violation of the rights of the claimants. The general and undifferentiated nature of the storage of fingerprints, biological samples and DNA profiles of individuals suspected of having committed crimes, but not convicted, does not constitute a fair balance between the public interests of national authorities and the private interests of those concerned: furthermore, the United Kingdom has overstepped any possible margin for leeway in the matter. The ECHR did not examine the criticisms made by the claimants regarding certain aspects of the data storage, such as the ease of access to these data, too great according to them, and a lack of protection against improper use and abuse. "Therefore, the disputed storage can be considered a disproportionate violation of the claimants' right to privacy and cannot be considered necessary in a democratic society".

Among these democratic States, a comparison can be made between the United Kingdom and France.

In the United Kingdom, the DNA database was created in 1995, but only for criminal cases. In France, the FNAEG (*Fichier national automatisé des empreintes génétiques*) DNA database was set up by Guigou law of June 18, 1998[40] exclusively to gather genetic fingerprints of individuals involved in crimes of a sexual nature.

In the 21st Century, offences for which genetic material is taken are increasingly frequent. In the United Kingdom, the law changed in 2001 and again in 2004. Since 2004, the DNA of individuals involved in any way in

39 CEDH, December 16 1999, no. 247224/94, T c/United Kingdom, sections 75 and 85.
40 ECHR and not CEDH.

an offence can be kept for an unlimited amount time by police and tracked, and retrieved anywhere in England, Wales or Northern Ireland.

In France, article 706-55 of the penal procedure code defines the cases in which DNA material can be taken and stored: for individuals convicted of any of the offences mentioned in article 706-55 of the penal procedure code, for individuals against whom serious evidence can be held and possibly lead to a conviction, for individuals who are reasonably suspected of having committed a crime or an offense. Furthermore, according to article R. 53-10 of the penal procedure code, it is also possible to take a sample in the following scenarios: biological traces from unknown individuals are collected as part of a preliminary inquiry, the investigation of a crime or obvious offense, or a preliminary investigation; biological samples are taken from unidentified corpses and biological traces are taken from unknown individuals; they are gathered in the context of an investigation into the cause of death, or as part of the search into an unsolved disappearance; biological samples coming from an individual declared missing, and collected as a part of an investigation into an unsolved disappearance; biological samples are taken, with consent, from the relatives of a missing person, as part of an investigation into unsolved disappearance.

The databases reflect the size of the phenomenon. The United Kingdom has the larger database, with 4.3 million genetic fingerprints in 2008, with at least 850,000 belonging to witnesses, victims or individuals not pursued by the courts or acquitted.

The genetic fingerprints that are stored are therefore particularly intrusive and the databases tend to get steadily larger. This is also true for centralized police files.

Technology is therefore used with increasing frequency to control the population.

To what extent has the emergence of digital technologies brought lawyers and politicians to use the controls to monitor not only the enemies of democracy, but a large part of the population.

Human rights are an ideology that is continuously evolving. Are these questioned through the use of this technology?

The goal of this book is to determine whether the balance between public order and the preservation of fundamental rights is still achievable today, when it would seem the side of security is currently winning it. This is not a theoretical study, but rather an empirical one. It draws on law, and to a certain extent political sciences.

The diachronic aspect of the question is highlighted: first the mythical time period when public order and privacy lived alongside each other shall be discussed.

Secondly, this book shall examine the time period around the start of the 21st Century, marked by an apparent victory of security, with its economic, financial and legal aspects, over the utopia of human rights.

Lastly, after the economic crash of 2008 comes the current era where the dominance of security clashes with ideas of jurisprudence, which come back into touch with the fundamental text relating to human rights.

PART 1

Technology and Human Rights

For a long time, technologies have been developed without any thought for ethical considerations. They remained external to international and economic law.

The notion of "human rights" did not appear to have any link to technologies and States.

Security and Privacy in the Digital Era, First Edition. Claudine Guerrier.

1

The Ideology of Human Rights

The technologies in the 20th and 21st Century, must respect human rights. But human rights correspond to a conception of beings and things that took a long time to build.

1.1. Constitutional texts

These texts have not always been an essential part of international or national law, far from it. For a while, only the United Kingdom was interested in protecting a suspected offender against arbitrary detention, notably with *habeas corpus*[1]. Human rights correspond to an old philosophical aspiration but they only entered the political sphere in the 18th Century, with texts of constitutional value, attached to the States, the French Declaration of Human Rights and the Citizen, the US constitution and its amendments.

I) *The Declaration of the Rights of Man and of the Citizen*

This emerged as part of the philosophy of the Enlightenment, encompassing a number of philosophical works, notably by Rousseau and Diderot, such as the Encyclopedia.

1 1679.

Security and Privacy in the Digital Era, First Edition. Claudine Guerrier.

The rights declared are rather numerous. The first[2] rights are freedom and equality, inseparable in nature. These are freedom and equality as rights, not as achieved concepts. However, freedom and equality as rights are the foundation for many other rights, listed in part in the Declaration of the Rights of Man and of the Citizen, and then later in future texts pertaining to civil law

A) *Freedom*: freedom is defined in a very broad manner. Everything that is not prohibited by the law is considered to be a freedom. Article 5 states: "The law can only protect against actions that are detrimental to society". All actions that are not made illegal in the law are included in the vast domain of freedom.

The Declaration of the Rights of Man and of the Citizen focuses particularly on the freedom of opinion[3] and the freedom of expression. The freedom of opinion encompasses all ideas, "even religious". This notion of "even religious" refers to the importance of religious opinions in the society of the 18th Century. The principle of royalty was founded on religion and its church (Catholic), and later its churches (since the Edict of Nantes). The King's legitimacy arises largely from his crowning, a religious ceremony. However, in the 18th Century, a number of men were able to separate themselves from the influence of religious opinions, either by freeing themselves from the concept of God (atheists remained a minority, however, who rarely expressed their beliefs; Libertines, such as Voltaire and D'Holback, were rather discrete on the matter of their atheism or their agnosticism) or by adopting a faith that was separate from the ecclesiastic institutions[4]. The constituents made progress by separating the world of politics from religion. Consequently, the revolutionary governments went after refractory priests refusing to swear allegiance as required. Robespierre, however, attempted to impose a new spiritualist institution by proclaiming a worship of the Supreme Being. Later the Empire re-established the influence of the churches. However, the work of the Declaration has survived, providing a foundation for the legal basis of freedom of opinion.

2 Article 1.
3 Article 10.
4 La Profession de foi du… Vicaire Savoyard (J-J Rousseau).

Freedom of opinion is not sufficient. It must continue to include freedom of expression[5]. This corresponds to the freedom to express ideas and opinions. Citizens attempt to share their ideas with other citizens, and this freedom of exchange is carried out through a number of media: speech (in later centuries through radio or television), writing (pamphlets, books, newspapers) and, since no one at the time could envisage electronic writing, social media, Internet and print. In this way, freedom of expression results in the freedom of the press through the right to print diverging or converging ideas. The first years of the revolution were marked by a huge rise in the freedom of the press, with a large diversity of opinions, marked by an underlying freedom of tone.

The power to detain, a privilege of public orders forces, is greatly limited. The law anticipates offenses, and the curbing of freedom caused by an arrest is anticipated by the lawmaker: "No man can be accused, arrested or detained unless in the manners prescribed by the law"[6]. The presumption of innocence is stated here[7]: "Any man is presumed innocent until proven guilty, and if it is deemed necessary to arrest him, any severity that is not needed to accomplish this shall be duly reprimanded by the law".

The last freedom joins the first, proclaimed as solemnly[8]: this is the right to property, presented as "inalienable and sacred". The right to property belongs to both civil law and economic law.

B) *Property*: exemptions are provided. Limitations to civil rights are envisaged by the law. Even property can be suspended "when public necessity, legally determined, requires it, and in exchange for a fair compensation beforehand".

The Declaration of the Rights of Man and of the Citizen is actually included in the constitutional texts of the Fifth French Republic in the same way as the *Preambule de la Constitution* of 1946, and the *Chartre de l'Environnement*. They participate in the constitutional control process carried out by the constitutional council, either beforehand (referral to the

5 Article 11.
6 Article 7.
7 Article 9.
8 Article 17.

Constitutional Council before the passing of a law) or afterward, since the 2008 reform with the question of constitutional priority.

Thus, the constitutional council came to the decision that certain nationalizations planned by the Pierre Mauroy government went against article 17 and violated inalienable and sacred principles of property.

The question of constitutional priority has several times looked into the correct application of freedom of opinion and freedom of expression. As a result, labor unions are allowed to distribute tracts without permission from the employer. This is not the case for electronic tracts, which require approval from the employer, unless an overall agreement is found. The priority issue of constitutionality (QCP) on September 27, 2013[9] declared that the Internet contains various networks that a company needs to monitor to some extent, and therefore the employer's authorization could not be considered an impingement of the freedom of expression as claimed by the CFTC.

Beyond the French constitution, the Declaration of the Rights of Man and of the Citizen has been a source of inspiration for all those reflecting on human rights in an international context.

II) *The other constitution/reference is the American Constitution of September 17, 1787*. The first 10 amendments make up the Bill of Rights; they were put forward by the First Congress on September 25, 1789 and ratified on December 15, 1791. The Declaration of the Rights of Man and of the Citizen and the Bill of Rights appeared at the same time. However, while the Declaration of the Rights of Man and of the Citizen lists the rights of French citizens, the Bill of Rights does not list the rights of citizens, but instead lists actions that the American Federal State cannot carry out on its citizens.

A) *The first amendment of the constitution covers freedoms*: freedom of opinion, freedom of expression and freedom of assembly. Regarding civil freedoms, the first amendment stresses the importance of the freedom to practice one's religion. The constituents are very attached to religious convictions and faith, even though the first Americans – the descendants of

9 QPC 2013-345.

Protestant colonists – were supporters of the freedom to choose religion. The American constitution contains many references to religion, and the President of the United States still swears an oath on the Bible when they take up their duties. Furthermore, in court citizens also swear an oath on the Bible. However, this freedom of opinion and expression is not limited to religion. All opinions can be held by American citizens, and they cannot be worried about showing their attachment to one or the other. This is why the freedom of the press cannot be limited. On this point, there is a dichotomy between the concept of the freedom of man and the citizen and the concept of freedom in the first amendment to the American constitution.

In France, revisionism is illegal and there are no revisionist websites. On the contrary, in the United States, where pro-Zionist lobbies are key in American politics, and where the United States is the unconditional allies of Israel in all and every context, revisionist websites are flourishing.

B) *The other amendments*: the fourth amendment concerns trespassing and illegal searches: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized". In the common law country, that is the United States, jurisprudence regarding the fourth amendment is sizeable.

The sixth amendment pertains to the rights of the accused. Suspects have the right to be defended and the jurisprudence relating to this stresses the importance of the role of lawyers[10].

The American constitution and its amendments[11] have had particular influence on common law countries. The American constitution is the product of a philosophical and political movement that survived the American Civil War[12] and later the political and military events that marked the 20th Century.

10 May 26, 2009: Montejo/Louisiana (presence of lawyers during police interrogations).
11 The first 17 amendments correspond to the Bill of Rights.
12 The Confederate States had adopted a constitution inspired by the Constitution of the "Northern States".

The movement supporting human rights, which appeared in the constitutions of the 18th Century, became widespread after the Second World War in the context of the creation of the United Nations.

1.2. Some texts have an international scope

This is the case for the Universal Declaration of Human Rights of the International Covenant on Civil Rights. The UN set up a new world order after the Second World War. It followed the objectives of the League of Nations, but in a different context, as the defeat of the Germany/Italy/Japan Axis led to the fall of a number of values that were no longer acceptable. The United Nations Charter, signed June 26, 1945, reaffirms its "faith in fundamental human rights, in the dignity and worth of the human person" and invites member States to enforce "respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion". The members of the drafting committee came from different nations: Eleanor Roosevelt (USA), Peng Chun Chang (China), Charles Habib Malik (Lebanon), William Hodgson (Australia), Hernan Santa Cruz (Chile), René Cassin (France), Alexander E. Bogomolov (USSR), Charles Dukes (United Kingdom) and John Peters Humphrey (Canada). Out of the 58 participating countries, 48 voted in favor of the Declaration of Human Rights and eight abstained. Some reasons are geopolitical: citing the principle of universality as stated in article 2 (oriental block: USSR, Czechoslovakia, Poland, Yugoslavia). Some reasons are linked to actual resistance regarding some principles of the Declaration. Saudi Arabia, protector of the Walhabi faith, was not convinced of the equality between men and women. South Africa was not convinced of the equality between races. Two other states did not partake in the vote: Yemen and Honduras.

I) *The Universal Declaration of Human Rights is resolution 217 (III) A*. It has no value as a legally binding document, but it is a reference text, and has become increasingly known as new States become members of the UN, especially since the 1960s with the time of decolonization. In addition to the principles of freedom, which were already established, recognition of social rights were also added. Moreover, the UN Commission for Human Rights plays a considerable role, relaying knowledge of the Universal Declaration

of Human Rights to new Member States, which has already become very widespread throughout the 20th Century, even in States that are not yet ready to apply it.

A) *The first article proclaims the principles of freedom and of equal rights*, which were already present in the Declaration of the Rights of Man and the Citizen, and where some might recognize the work of the Frenchman René Cassin. The rights invoked are those of "human beings", meaning men and women, which explains the difficulties of some States to accept the Declaration, notably Saudi Arabia. The first article explains the reasons for this equality: human beings are endowed with "reason and conscience". This double term justifies the acceptance of the rights that are developed throughout the whole of the Declaration.

"Distinctions" are not permitted: a list is made up of these distinctions that should not be taken into account: race, color, sex, language, religion, political opinion or "any other opinion", national or social background, wealth, birth or "any other situation". These distinctions can in no circumstance lead to discrimination[13].

B) *Next the rights are listed*: right to life, freedom and safety. Slavery, servitude, torture, and "cruel, inhuman or degrading treatment or punishment" are all prohibited.

Articles 10 and 11 on the rights of the accused appear to be slightly influenced by certain amendments of the American constitution, but the presumption of innocence[14], inherited from the Declaration of the Rights of Man and of the Citizen, is also stated. The accused has the right to a defense. Article 12 is the first text that is a foundation of the respect of private life and the secrecy of correspondence: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation".

Other rights proclaimed are the right to free movement[15], the right to asylum, the right to a nationality and the right to have a family. Others include those at the center of the Declaration of the Rights of Man and of the Citizen: right to property, freedom of thought, conscience and religion. The

13 Article 7 of the Universal Declaration of Human Rights.
14 Article 11.
15 This implies the freedom to leave one's country, but also to return (article 13).

Declaration stresses the importance of religion and explains that freedom of conscience leads not only to the freedom to change religion (which is not accepted by certain religious faiths) but also to practice one's religion, share one's convictions and carry out rituals. Article 19 is dedicated to the freedom of opinion and expression "this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers". The right to assembly corresponds to article 20.

Next come the rights relating to the sovereignty of the people (which did not exist in the texts of the 18th Century) and to social rights.

Article 21 states that "The will of the people shall be the basis of the authority of government". This will of the people is seen in "honest" elections that must be held periodically, using equal universal suffrage, and with a secret ballot.

Social rights include the right to social security, the right to work, the right to rest and hobbies, the right to a minimum quality of life and the right to education.

The objective of social security is to allow the achievement of "economic, social and cultural rights indispensable for his dignity and the free development of his personality"[16]. The right to work involves free choice of the work and protection against unemployment[17]. "Everyone who works has the right to just and favorable remuneration ensuring for himself and his family an existence worthy of human dignity, and supplemented, if necessary, by other means of social protection". The freedom to join unions is guaranteed.

The right to rest is based on a limit on the amount of time worked (maxima, deadlines) and on periodical paid vacation.

A sufficient quality of life is also a fundamental right[18]; this must allow every individual and their family to have access to food, clothing, shelter, medical care, social services, security in the case of "unemployment, sickness, disability, widowhood, old age or other lack of livelihood".

16 Article 22.
17 Article 23.
18 Article 25.

Motherhood, as well as children "whether born in or out of wedlock", are protected.

Education combines a vision that is both secular and religious. For religious reasons, the parents are at the center of the choice of education. For reasons of secularism, education is free "at least in the elementary and fundamental stages", making it obligatory to a degree. Higher education is encouraged and must be accessible on a basis of equality and meritocracy.

These social rights are largely challenged nowadays by certain States and companies for reasons of the priority given to competition in commercial societies, limiting access to social rights and social protection: most of the reforms advised by the IMG, the OECD, or even the Union European ask for a reduction of public spending on schemes meant to increase the happiness of the majority of citizens.

Indeed, the International Labour Office (ILO) claims that globalization is compatible with its conventions, but most employers' organizations in the majority of States are against the ratification of ILO conventions. Otherwise, when the conventions are ratified, they tend to demand the convention be denounced so that companies are able to deal with competition properly, as was the case in France with Convention 158 of the ILO, which makes it obligatory for there to be a reason behind a redundancy, with an appeal and compensation available. Whatever the ILO might think, it seems globalization presents a threat to the rights "acquired" by employees in developed countries, since globalization provides access to very cheap labor in less developed countries.

The Universal Declaration of Human Rights, while non-binding, is referenced by all individuals, physically and morally, who have a direct or indirect attachment to human rights.

II) *The International Covenant on Civil and Political Rights*[19] was adopted by the General Assembly of the UN in resolution 2200 A (XXI). The Universal Declaration of Human Rights was written in French. The International Covenant on Civil and Political Rights is written in English, Chinese, Spanish and Russian. The Pact is binding for States that have

19 PIDCP.

ratified it. As the name suggests, it focuses on the first group of concepts covered by the Universal Declaration of Human Rights, which are civil rights. It came into force on March 23, 1976, after 35 instruments of ratification had been obtained. The first part, made up of the first article, focuses on peoples. The second part lists the civil and political rights that the State is committed to protecting.

A) *The first article states that different peoples have the right to self-determination*. These peoples determine their political status and their methods of economic and social development.

B) *Individuals (in this work, this is not the same as "citizens" and "persons") have their own rights in the same way as peoples do*. No distinction can be made based on race, color, gender, religion, political or other opinion, national or social origin, wealth or birth that would change the rights of individuals recognized by the State. This is why States guarantee remedies for individuals if their rights are violated. If an exceptional public danger threatens the very existence of the nation, States may need to adopt derogatory measures with regard to the covenant, as long as these measures are compatible with international law and do not engender discrimination based on race, color, gender, language, religion or social origin.

All humans have a right to life and the covenant is in favor of abolishing capital punishment. In States where this punishment still exists, it can only be carried out for the most heinous crimes. The death penalty cannot be given to minors, and pregnant women cannot be executed. Torture, inhumane, cruel and degrading treatment are prohibited. Individuals must not be subjected to medical or scientific experimentation. Clearly the memory of the eugenics programs carried out by Nazi Germany on individuals with mental disabilities in concentration camps during the Second World War was fresh in the minds of the authors of the covenant.

Slavery and servitude are forbidden. Forced labor is regulated and monitored. Generally, forced labor as a punishment is not allowed. Forced labor can, however, complement a punishment of imprisonment, as long as it is ordered by a court. The following are not considered prohibited forced labor: work or services required of an inmate following a legal order or on conditional release; military service, and, in countries where conscientious objection is permitted, the relevant service required for conscientious

objectors; service required in the case of disasters or emergencies; work or services that constitute normal parts of obligatory civil duties.

All individuals have a right to freedom and safety. Arbitrary arrests and detention are not permitted. Any individual who is arrested must be notified of the accusations made against them. Arrested individuals are treated "with humanity and with respect for the inherent dignity of the human person"[20]. Upmost efforts are made to keep defendants and inmates separate during detention, and young defendants must be kept separate from adults. The presumption of innocence is solemnly stated: "Everyone charged with a criminal offence shall have the right to be presumed innocent until proved guilty according to law"[21]. The rights to a defense are guaranteed.

Each individual has the right to legal personality. The rights to free movement, private life and the freedom of thought, conscience, opinion and assembly are all guaranteed.

Freedom of movement implies the freedom to move freely within a State, to choose a residence and to leave countries, including one's own. The exceptions made to this principle aim to protect national security, public order, health and public morality. Foreigners must not be expelled from the country, except for compelling reasons of national security, and they should have the opportunity to file an appeal.

The right to privacy[22] leads to a similar approach as that of the Universal Declaration of Human Rights: there can be no interference with privacy, whether at home, as a violation of the secrecy of correspondence, or as an attack on honor or reputation[23].

The freedom of consciousness focuses mainly on religious freedoms, leading to several subclauses. Religious freedom implies the freedom to choose religion, to express one's religious convictions "individually or in community with others"[24], in public or privately through worship, rituals,

20 Article 10 of the International Covenant on Civil and Political Rights.
21 Article 14.
22 Article 17.
23 Essentially, this targets libel and slander.
24 Article 18.

dogma and teaching. States aim to respect the choice of parents and legal guardians with regard to the religious and moral education of children under their care, in line with their own convictions. This approach, at a time where State atheism is the legal *status quo*, corresponds to a western position, if not an American one, but is also in line with the aspirations of muslim States.

Everyone has the right to freedom of opinion and expression. Freedom of expression includes the freedom to research, receive and spread information and ideas orally through writing, print, artistically or in any other format.

The right to peaceful assembly is recognized: this can only be limited in the interest of national security, public security and public order. Freedom of association and the freedom to membership of a trade union are protected.

While men and women are considered to be equal, the covenant stresses the importance of family in the listing of rights. Article 23 goes as far as stating[25]: "The family is the natural and fundamental group unit of society and is entitled to protection by society and the State". Individuals of "marriageable age" are granted the right to marry and to start a family[26]. Marriage can only be entered with the full consent of the intending spouses.

Children have the right to[27] "such measures of protection as are required by his status as a minor, on the part of his family, society and the State". Children are registered from birth, and have the right to a name and a nationality.

"Ethnic, religious or linguistic" minorities[28] cannot be denied by the State the right, in common with other members of their group, to have their own cultural life, to profess and practice their own religion, or to use their own language.

These rights are not only principles, they are defined in detail and the guarantees established can give rise to minute accommodation, especially in the domains that play an important in the covenant, such as religion

25 The influence of religion, omnipresent throughout the covenant, is particularly present in this article.
26 It led to various different – sometimes divergent – interpretations.
27 Article 24.
28 Article 27.

and family. Solutions are often provided in the case of violations of these rights.

For this reason, the creation of a Human Rights Committee[29], to ensure these rights are not violated, is unsurprising. This Committee consists of citizens of the ratifying States: these individuals are held to be competent on the subject of human rights: some have experience in the legal field. The members of the Committee are elected by secret ballot from a list of people fulfilling the criteria mentioned above, presented by the ratifying States. To ensure the independence of the committee, one State can only be represented by a single person[30] (the Committee comprises 18 representatives); during elections, an attempt is made to consider a very diverse geographical distribution, as well as the desire to represent various forms of civilization and the main legal systems (notably common law, roman law).

By the end of January 2015, the covenant had been ratified by 168 States. The United States ratified it in 1992 with a number of conditions, making parts of it non-binding on the American soil. For example, article 20 of the covenant, listing exceptions to the right to spread ideas, prohibits pro-war propaganda and the inciting of racial or religious hatred. This limitation, which is accepted within the European Union, goes against the first amendment of the United States constitution. France has also expressed reservations, with regard to article 27, in the name of Republican universalism. The French Republic is "one and indivisible", and minorities have no special rights. In fact, in France classifications based on ethnicity or on the concept of minorities are prohibited. In 2008, the UN Economic and Social Council asked France[31] to remove this reservation, but the recommendation was not followed up.

Two successive protocols were added to the covenant. The first of these establishes a mechanism to be used following a complaint concerning a violation of the covenant by a ratifying State. This protocol came into force on March 23, 1976. The second protocol prohibits the death penalty. It came into force on July 11, 1991.

29 Fourth part.
30 Article 31.
31 "Observations faites à la France par le Comité des Droits économiques et sociaux", 4th session, 28 April–16 May, 2008.

The Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, while intended to have a universal reach, have been mainly influenced by the legal systems of democratic western countries.

1.3. European texts

Other more "operational" texts involve laws of general interest. Most notably, this is the case of the European Convention for the Protection of Human Rights and Fundamental Freedoms, an international treaty signed by the member States of the Council of Europe[32], and that came into force on September 3, 1953 in the context of a bipolar world: at the time the Member States of the Convention were all western countries, which stopped being the case after 1990.

I) *The European Convention for the Protection of the Human Rights and Fundamental Freedoms* refers explicitly to the Universal Declaration of Human Rights. Violations of the rights listed in the Convention are taken to the European Court of Human Rights by way of the State; if this violation has been committed by a State, the case is taken to the ECHR by the individual[33], which can only happen after all paths internal to the State in question have been exhausted.

The following rights and freedoms are listed:

A) *Among these rights are the right to life, the prohibition of slavery and forced labor and the right to safety*. Every person's right to life is protected. Death cannot be handed out intentionally, except as part of a sentence of the death penalty, which is later prohibited. Torture and inhuman or degrading treatment are not allowed. Even so, some States are to later be convicted of acts of torture: Turkey is one example. France, which only joined the Convention in 1974 and only allowed individual requests in 1981, effectively waited for torture to stop being a regular practice before ratifying the Convention[34]. Slavery and forced labor are prohibited. The exceptions made for forced labor (additional sentence to detention, military service,

32 The Council of Europe covers States located in the European continent that claim to adhere to democratic values. Turkey is a member, and, following the end of the Cold War, Ukraine and Russia also joined.
33 Article 56 of the Convention.
34 Cf: Algerian war.

service in the event of a disaster or crisis) are repeated in the International Covenant on Civil and Political Rights.

Individuals cannot have their freedom taken away, except in certain scenarios following legal pathways: imprisonment as a sentence given by a court; in the case of subordination; as a form of temporary detention; normal detention of a minor in a supervised educational facility; detention of a person likely to spread a contagious disease; detention of mentally ill individuals, alcoholics, drug addicts, vagrants; arrest and detention of an individual to stop them illegally moving in the territory of State or against whom extradition proceedings are ongoing. These exceptions are rather numerous and leave a large margin for discretion to the State. Nevertheless, a person arrested or detained is entitled to certain rights: they must be quickly informed of the reasons for their arrest, brought before a magistrate, judged within a reasonable timeframe or freed during the procedure. In the occurrence of arrests or detentions that go against the Convention, the victim must be able to obtain compensation.

The trial must be fair. The process is made public, except when the proceedings are not in the interest of morality, public order, national security in a democratic society or when they are against the interests of minors or protection of privacy. The individual accused is presumed to be innocent until they are proven guilty. The accused has the right to detailed information on the reasons for their arrest, provided in a language that is understandable by them; they have the right to an adequate defense, i.e. to help a defense of their choosing, or the free assistance of a state-appointed lawyer if the accused does not have the resources to pay for a lawyer themselves, and the free assistance of an interpreter, if the person is an alien.

B) Freedoms

Every individual has the right to privacy to freedom of thought, conscience, religion, freedom of expression, assembly and association.

Everyone has the right to the protection[35] of their privacy and family life, their home and their correspondence.

35 Article 8, often referred to.

Each has the right to freedom of thought, conscience and religion; this implies the possibility of changing religion and convictions, but also expressing one's religious or other convictions, alone or in public, through worship or teaching. The limits of the freedom to express religious or other convictions arise from measures necessary in a democratic society for public security, the protection of order and the protection of the rights and freedoms of others.

Freedom of opinion implies the right to receive or share information or ideas without interference from public powers, which can, however, exert some level of control over radio or television stations.

Everyone is entitled to the freedom of peaceful assembly and association, including the right to belong to a trade union.

Each person of a marriageable age has to the right to marry and start a family.

These rights and freedoms are guaranteed without any distinction made based on gender, race, color, religion, opinions, national or social origin, belonging to a national minority, wealth or birth. Discrimination is strictly prohibited. Violations of rights are also prohibited.

However, States can make exceptions on the basis of the principle of proportionality. This is the case for security, most notably national security. In this way, France informed the Secretary General of the Council of Europe on November 24, 2015 that some exemptions would be made[36] to the European Convention for the Protection of Human Rights during the state of emergency for reasons of national security. The question is do certain actions carried out in the name of a state of emergency go beyond the context of the terrorism warranting the state of emergency in the first place?

C) *Additional protocols have been adopted*

Protocol number 1 relates to property, education and elections: private property is protected (taken from the Declaration of the Rights of Man and of the Citizen). Parents decide on the methods of education for

36 No exemptions are possible for articles 2 (right to life), 3 (prohibition of torture), 4 (no slavery or servitude) and 7 (no sentence without a law).

their children in line with their religious or philosophical convictions. Citizens have the right to present themselves in the context of free and regular elections.

Protocol number 4 prohibits the imprisonment of individuals "on the ground of inability to fulfill a contractual obligation". The expulsion of nationals of a State from that State is prohibited, as is the collective expulsion of aliens. Most importantly, article 2 of protocol four guarantees freedom of movement within a country, as well as the right to leave the country.

Protocol number 6 abolishes capital punishment during times of peace[37] and is discussed in detail by a large number of States. Protocol number 7 concerns expulsion, appeals regarding penal matters and equality between spouses: article number 1 prohibits the expulsion of "lawfully resident" aliens, unless the law decides differently, and even in this case the aliens in question have a right to know the reasons for their expulsion and may ask for their case to be reexamined. This protocol also refers to family and states the equality of spouses.

Protocol number 12 extends the ban on discrimination to all legal rights, even if they are not present in the Convention, as long as they are present in a national text.

Protocol number 13 calls for the complete abolition of the death penalty, both during times of war and peace. This protocol has not been ratified by all States, although it would be accurate to say that the countries of the Council of Europe do not have capital punishment, as it is not applied. Nonetheless, discussions are ongoing, and some political parties in several member States of the Council of Europe that have ratified protocol number 6 and sometimes 13 demand the repudiation of these protocol and the reestablishment of the death penalty. This is one of the most widespread topics of discussion along with immigration and security.

These protocols have been ratified.

For this year protocols 15 and 16 have not been ratified. Protocol number 15 seeks to reduce the number of individual requests made to the European

37 In this protocol, the death penalty can only be carried out in times of war or in a state of emergency.

Court of Human Rights by involving national judges in applying the Convention during the appeals process. France signed protocol number 15 on June 24, 2013, but has not ratified it. By the end of 2014, 10 out of 47 States had ratified this text.

Protocol number 16 covers the optional jurisdiction of the European Court of Human Rights. An assent procedure is set out and is available to the highest national courts. It covers theoretical questions on the interpretation and application of the rights and freedoms mentioned above. By the summer of 2014, 14 States had signed the protocol, but so far no State has ratified it.

For our subject matter, the main references are article 8 on the right to privacy and the secret of correspondence, and article 2 of protocol 4 on the freedom of movement.

There is a link between the European Convention for the Protection of Human Rights and Fundamental Freedoms and the laws of the European Union. The UE is not a member of the Convention, as it did not possess legal personality at the time of creation of the Convention. However, the Treaty on European Union states in article 6: "the Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms… Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law". Furthermore, all Member States of the Union have ratified the Convention. Moreover, in 2005 the European Court of Human Rights declared itself competent to verify the conformity of the acts of application of norms emanating from European Union law[38].

II) *The European Charter of Human Rights*: at the level of the European Union, there is a specific body that deals with human rights, largely inspired by the Declaration of Human Rights and the International Covenant on Civil Rights. This is the Charter of Fundamental Rights of the European Union, a bill of rights adopted on December 7, 2000. The Treaty of Lisbon in 2007 incorporated the Charter into the article covering fundamental rights and aims to make it binding; this aspect was met at the start with reservation

38 Bosphorus judgment; ECHR, June 30, 2005, 45036/98.

from Poland and the United Kingdom. Since then, Donald Tusk has expressed Poland's intention to fully adhere to the Charter.

The process was the following: the European Councils of Cologne[39] and Tampere[40] gave a mandate to a working group regarding the creation of a project regarding human rights. The European Council of Biarritz[41] gave its unanimous consent to the project; on November 14, 2000, the European Parliament adopted the Charter and the Commission granted its approval on December 6, 2000.

The presidents of the European Parliament, Council and Commission signed and proclaimed the Charter on December 7 in Nice. The Charter was then solemnly proclaimed on December 12, 2007 during a ceremony at the European Parliament in Strasbourg. This was an achievement as since the Nold judgment[42], fundamental rights recognized by the laws of Member States, are part of the right of communities.

The Charter of Fundamental Right of the European Union contains a unique text listing all of the civic and social rights of European citizens: this text is also valid for all individuals living in the territory of the European Union.

Since December 2009 and the coming into force of the Lisbon Treaty, the Charter of Fundamental Rights of the Union has acquired obligatory legal powers, identical to those of treaties. Article 6(1) TUE states: "The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties".

The Charter applies to the three European pillars. The Charter is also a reference for activities launched by the Union Agency for Fundamental Rights, set up in February 2007.

This agency has the following three main missions:

– to gather information and data;

39 June 3 and 4, 1999.
40 October 1999.
41 October 13 and 14, 2000.
42 Judgment of the Court of Justice of European Communities May 14, 1974.

– to provide advice to the European Union and its Member States;

– to favor dialog with civil society in the domain of fundamental rights.

In the French version of Charter 2000/C 364/01, the first word of Chapter 1 of the charter is “Dignité”.

A) *Rights*: dignity includes human dignity, the right to life, the right to the integrity of the individual and the prohibition of torture, slavery and forced labor.

Human dignity is inalienable[43]. It must therefore be protected and respected: this is the essence of article 1 of the Charter.

The right to life implies the abolition of the death sentence and the prohibition of executions. The abolition of the death penalty is therefore an integral part of the principles of the Charter.

Individuals also have a right to human integrity: this concerns mainly medicine and health. Eugenics, notably practices aiming to carry out selection, is prohibited. Making a profit from the human body or from any of its components is forbidden. This implies a ban on organ trafficking, as well as on surrogate mothers when they revolve around a monetary contract. The reproductive cloning of humans is also illegal. This section is particularly interesting for medical research and its problems that could be potentially justified in the name of science and omnipotent consumers.

The following are also prohibited: torture, inhuman or degrading treatment, slavery and forced labor, including derogatory labor as it also appears in the International Covenant on Civil Rights.

B) *Chapter 2 is dedicated to freedoms*. Some of these freedoms that appear in older texts are universal; others are new for this type of document, such as the protection of personal data.

Everyone has a right to privacy and the protection of their family life, their home and their communications[44].

43 It is afforded the same status as property is given in the Declaration of the Rights of Man and of the Citizen in 1789.
44 The term “communications” replaces the traditional term “correspondence” .

Everyone has a right to the protection of his or her personal data. These data are treated with loyalty, with a defined objective and on the basis of consent given by the person in question. Every individual has the right to access and rectify these data. This is controlled by an independent authority.

These statements are nearly identical to those of the UN General Assembly resolution of December 14, 1990 of Convention 108 of the Council of Europe, and directive 95/46 of the European Union. However, while all these sources of law looked into the protection of personal data, they were never meant to be the basis for fundamental rights. In the 21st Century, personal data are therefore presented in the Charter as representing an issue of personal freedoms. In the era of "Big Data", while public authorities seek to defend security by gaining a privileged access to some data, and while moral individuals in private law consider data files as being an essential part of their business, this vision is realistic but also reflects a very European approach, as the points of view of the United States on the matter is very different.

Articles 9 and 10 are more conventional. Everyone has the right to get married and start a family: there is no mention of a "marriageable age", but instead guarantees are made regarding national laws. It is therefore the principle of subsidiarity that applies.

Each individual has the right to freedom of thought, conscience and religion. Religious freedom involves the freedom to change religion; moreover, the freedom of conscience and religion implies the ability to express one's religion or convictions, individually or collectively, publicly or privately.

The right to conscientious objection is recognized[45] but governed by national laws, here too depending on the type of subsidiarity.

The freedom of expression[46] encompasses the freedom of opinion and the freedom to receive and express ideas; the article states that there can be no interference on behalf of public authorities, which is highly useful. The

45 Article 10, paragraph 3.
46 Article 11.

freedom of the media (no longer press, but media) is guaranteed, and pluralism is respected. This freedom is both a civic and economic freedom; jurisprudence has shown that the economic and civic aspects of this freedom are not easily reconciled as economic freedom involves the search for maximal profit, while the freedom to express minority opinions in a medium can be problematic economically and civically.

Everyone has the right to freedom of peaceful assembly and association at "all levels", in all "political, trade union and civic matters"[47], which results in the freedom to join trade unions for the protection of one's interests.

Political parties at Union level contribute to expressing the political will of citizens of the European Union. The ability to aid in the expression of the will of the people appears in the constitutions of several member States, including France[48].

Article 13 is quite original: it states that the arts and scientific research are free; this means that both the arts and research cannot be given fixed objective by public authorities.

Each person has the right to education. This involves the possibility to receive compulsory education; public primary and secondary education that does not seek to make a profit must be available; registration fees can be more or less high. However, public education exists alongside other forms of teaching, as the covenant proclaims the freedom to create educational establishments and the right of parents to choose for their children a form of education in line with their religious, philosophical[49] and pedagogical beliefs, which is relatively innovative, in which – despite the diversity of pedagogical methods trialed during the 20th Century – pedagogical diversity had never been considered in reference texts on human rights.

Next are the freedoms that are halfway between civil and economic rights: professional freedom, entrepreneurial freedom, right to property and right of asylum.

47 Article 12.
48 "Les partis politiques… concourent à l'expression du suffrage", Constitution of 1958, article 4.
49 It features in the international treaties covered previously.

Every person has the right to work and a "freely chosen or accepted occupation"[50]. The search for employment is carried out over the entirety of the territory of the European Union.

Entrepreneurial freedom refers to both to community law and national laws. Every person has the right to property. Public utility can limit this right, but in this case fair compensation must be given. This principle of compensation in the case of nationalization has become a rule in western countries, especially following the nationalization of the Suez Canal by Egypt, and the ensuing violent reaction from the United Kingdom and France[51]. The use of goods can be regulated by the law "in so far as is necessary for the general interest". Intellectual property is recognized and protected.

The right to asylum is guaranteed in line with the Geneva Convention on July 28, 1951 and protocol 1067 on January 31 regarding the status of refugees.

Collective expulsions are prohibited, and no one can be expelled or extradited to a State where fundamental rights are not respected, where the person in question is likely to face the death penalty, torture or inhumane or degrading treatment.

C) *Chapter 3 is called "equality"*. The main principles are of non-discrimination, equality between the sexes and the rights of children.

All individuals are born equal in right, going back to the very old axiom of the Declaration of the Rights of Man and of the Citizen on 1789.

All forms of discrimination are forbidden, especially when they aim to make distinctions between gender, race, color, social or ethnic origins, genetic characteristics[52], language, religion, political or other opinions, wealth, birth, disability[53], age, sexual orientation[54] or nationality.

50 Article 15.
51 Called a "confiscation" by the UK and France in 1956.
52 It does not appear in older texts.
53 The prohibition of discrimination based on disability appeared at the end of the 20th Century.
54 Like disability, this also appeared at the end of the 20th Century.

Equality between men and women is guaranteed in all areas including employment, work and pay. This principle of equality does not exclude the adoption of measures to help represent the underrepresented gender (currently the female gender). This explains the measures taken in some countries for the benefit of parity, aiming to increase the representation of women in legislative assemblies[55].

Children have a right to protection and care that is vital to their wellbeing. This justifies the work of social services when the family is found to be lacking or abusive. Children can express their opinions freely. These opinions are taken into consideration regarding matters that concern them, depending on their age and maturity. The effectiveness of this requirement is not clear, especially when it conflicts with other rights, especially family rights. In nearly all States of the European Union, magistrates favor the link between child and parent, whatever the parent's behavior toward the child may be. Regarding questions of custody, when a child expresses the desire to sever relations with one of his or her parents, this is hardly ever respected, regardless of the age or maturity of the child. However, paragraph three of article 24 states: "every child shall have the right to maintain on a regular basis a personal relationship and direct contact with both his or her parents, unless that is contrary to his or her interests". Judges hardly ever consider this contact to be "contrary to his or her interests".

Chapter 3 focuses on the rights of elderly people, a growing demographic within the European Union, and on the rights of disabled people. "Equality" is here linked to the preservation of dignity.

Chapter 4, dedicated to "solidarity", proclaims social rights, the right to collective negotiation, right to strike, protection against unjustified dismissal, limits to maximum working hours, the right to daily and weekly periods of rest[56], the prohibition of the employment of children, the right to social security and the protection of health, access to services of general economic interest and the protection of the environment of consumers.

55 This is the case in France.
56 The right to a weekly rest, and not specifically Sunday rest, directive 93/104 on November 23, 1993.

Chapter 5 is dedicated to citizenship. Everyone has the right to vote and is eligible for election to the European Parliament in the Member State where he or she resides. The members of the European Parliament are elected by direct universal suffrage in a free and secret ballot[57]. The citizens of the European Union also have the right to vote and stand in municipal election in the Member State where they reside.

Article 45 proclaims the freedom of movement and residence in the territory of the Member States. The Schengen area was established through the Agreement and Convention signed between 1985 and 1990.

Chapter 6 is dedicated to justice.

Every individual has the right to an affective remedy before a court of law. They must be heard fairly and publicly, and have the possibility of being aided by a defense. Legal aid is therefore obligatorily provided for individuals without the means needed to cover the costs of their defense.

The accused is presumed innocent until they are proved to be guilty by a court of law.

No one shall[58] "be held guilty of any criminal offence on account of any act or omission which did not constitute a criminal offence under national law or international law at the time when it was committed. Nor shall a heavier penalty be imposed than the one that was applicable at the time the criminal offence was committed". The severity of the sentence is determined based on the severity of the crime.

No one can be put on trial or punished for a crime for which he or she has already been acquitted or sentenced within the European Union.

An explicit reference is made to the European Convention for the Protection of Human Rights and Fundamental Freedom. Since the Charter reuses some rights that are present in the European Convention for the Protection of Human Rights and Fundamental Freedoms, the mean and scope of these rights are the same as those provided in the Convention. This does not stop the Union establishing rights with a broader reach.

57 Discussions on electronic voting, which is not used for European Parliament elections.
58 Article 49.

The Charter is effectively in line with the Convention, and it covers relatively recent concepts. It supplements certain rights and freedoms with regard to the progress made in human and social sciences in the past 20 years. It reflects European culture and values, and is more advanced in some domains than the texts that came before it.

Beyond and in addition to these rules, some non-governmental organizations have conducted work in the matter of human rights, notably in the United Kingdom and in the United States. ACLU[59] and Privacy International have conducted considerable efforts in the defense of freedoms.

ACLU is an American not-for-profit organization based in New York whose goal is to defend the individual and collective freedoms guaranteed in the American Constitution and in the laws of the United States. It forms a lobby of sorts in terms of civil rights, providing information in terms of new dangers that are likely, with time, to threaten the fundamental rights of Americans, and sometimes carry out actions in court. The work conducted by ACLU has resulted in the evolution of a number of aspects of constitutional law. This organization is critical of both the Democrat and Republican Party. We shall return later to some of the battles of the ACLU, especially against the CIA and the NSA.

Privacy International was created in 1990, and was granted the status of not-for-profit organization in 2002. It focuses mainly on the problems relating to personal freedoms in the United States in the sector of electronic communication and private life.

In Europe, the EDRI[60] seeks to defend freedoms in the area of information and communications technology. Its members come from a large number of people from Western and Eastern Europe.

While these organizations have a very different approach to the treaties, they are highly vigilant and cannot be ignored in their actions to prevent those aspects of modern technology that might violate individual freedoms.

59 American Civil Liberties Union.
60 European Digital Rights is a not-for-profit organization.

2

Protection of Personal Data

Beyond the texts on fundamental freedoms, other important texts have appeared on the protection of personal data and computerized or automatic individual-related data.

The first text appeared in the United States, as informatics experienced a massive rise on the American continent. Despite this, the Privacy Act of 1974 was very modest and only considered public files.

Later, worries concerning privacy with regard to digitized files reached the European continent, leading to the first national laws in Germany, Sweden and France.

2.1. Convention 108

The first reference text with an international scope is Convention 108 from January 28, 1981 of the Council of Europe. The text refers to the protection of privacy[1] and seeks to protect the transmission of personal data processed automatically. The individuals concerned are physical persons, unrelated to their nationality and area of residence, but rather in the context of the Sates of the Council of Europe. Personal data are defined as the information relating to identified or identifiable physical persons.

1 Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

Security and Privacy in the Digital Era, First Edition. Claudine Guerrier.

Automated data files gather information that is then processed automatically.

I) *Automatic processing includes all of the following operations*[2] *"carried out in whole or in part by automated means*: *storage of data, carrying out of logical and/or arithmetical operation on those data, their alteration, erasure, retrieval or dissemination*".

Automatic processes are of interest as much in the private sector as in the public sector; lawmakers did, however, first focus on the public sector, inasmuch as in the 1970s and 1980s it was mainly public authorities that were at risk of violating rights to privacy via automatic processing[3].

II) *Convention 108 determines the ground rules in terms of protecting personal data*[4]: this is collected and processed fairly, and stored with clearly established and legitimate purposes. The data can in no case be used for reasons that are incompatible with the defined purposes. The data are accurate and correct, and can be updated if necessary. They are kept for a limited amount of time.

Some categories of data can only be processed automatically if internal legislation has established appropriate guarantees: this includes data that reveal racial origins, political opinions, religious or other convictions, and data relating to health or sexuality. These data must be granted a special form of protection.

The data are secured, and special care is given to the risk of accidental destruction, accidental loss, access, modification or unauthorized distribution.

Every physical person has rights regarding these personal data[5]:

– they are entitled to know about the existence of the automated personal data file, its purposes, habitual residence and the identity of the "controller of the file";

2 Article 2 of Convention 108, c.
3 Cf. Safari case in France.
4 Article 5 of Convention 108.
5 Article 8 of Convention 108.

– they are obtained at reasonable intervals and at no excessive cost, confirmation of the existence of the automated file, in an intelligible form[6];

– they can obtain rectification of the data or its erasure when the processing has been conducted in a way that violates the procedure established previously;

– they must have a remedy if a request for confirmation, communication, rectification or erasure is not complied with.

The cross-border flow of data is tied to the freedom of movement. A State is not within its rights to prohibit the cross-border flow of data or to submit them to a specific authorization if the sole reason is the protection of personal data. Exemptions to this rule are allowed for certain categories of personal data due to the nature of the data (see article 8 of Convention 108).

III) *Recommendations were added to Convention 108 during the 1980s*:

– Recommendation number R(81)1 on January 23, 1981 on the regulation of automated medical databases.

– Recommendation number R(83) 10 on September 23, 1983 on the protection of personal data used in scientific research and statistics.

– Recommendation number R(85) on October 25, 1985 on the protection of personal data used in direct marketing[7].

– Recommendation number R(90) 19 on September 13, 1990 on the protection of personal data used in payments[8].

Convention 108 contains provisions that are still applicable today. The work carried out by lawmakers and IT specialists in the Council of Europe has given a protective outline to personal data on the European continent.

2.2. United Nations General Assembly Resolution 45/95 on December 14, 1990

On the international level, this resolution has intervened on the leading principles of the regulation of digitized files containing personal data. UN

6 The encrypted form is excluded.
7 With this recommendation, legal persons under private law appear in an underlying manner.
8 The bank is at the forefront of the scene.

General Assembly resolutions are not legally binding, but certainly act as a reference. The focus is on the principles that must govern personal data.

I) *The main principles are lawfulness and fairness, purpose specification, access and non-discrimination*. Data cannot be obtained or processed in illicit or unfair ways, or used for purposes that go against the Charter of the United Nations.

Individuals responsible for setting up a file or applying it must check the accuracy of the data recorded and ensure that any mistakes are corrected, and that the file is up to date.

II) *Each file is created with a specific purpose*. The purpose of its use is specified, warranted and, during application of the file, made public in a way that it becomes known to the person concerned, so that it can be verified.

The individuals concerned have a right of access: they have the right9 to know if the data that relate to them are being stored or processed. They have the right for it to be communicated to them in an intelligible form, without excessive delay or cost, as well as the right to have rectifications made. In the case of rectifications, the cost is covered by the file controller.

Data that could lead to possible discrimination, particularly information regarding racial or ethnic origin, color, sexuality, political, religious or philosophical convictions, membership of a trade union, cannot be collected.

Security measures are envisaged to protect files against accidental loss or destruction during an accident.

When the laws of two or more countries provide similar guarantees regarding the protection of privacy, information corresponding to personal data circulates freely.

2.3. Sources of EU law

At the level of the European Union, opinion is divided: the United Kingdom wants general leading principles; Germany and France are seeking highly protective legislation in the sector of personal data.

9 Leading principle four.

I) *The more protective option is chosen in directive 95/46*[10]. The objectives are nearly identical to those of Convention 108 of the Council of Europe.

A) *Personal data are defined, as in Convention 108, as "any information relating to an identified or identifiable natural person*", but directive 95/46 has a number of additional clarifications: "an identifiable person[11] is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

B) *Information is processed fairly and lawfully*. It is gathered for specific, legitimate purposes and cannot be followed up with forms of processing that are incompatible with these purposes. Changes in purpose are prohibited. If a file or an automated data process is created with an objective in mind, this must be made known. In France, the penal code[12] is strict:

> "Anyone holding personal data at the time of its recording, classification, transmission or any other form of processing who diverts this information from its proper purpose, as defined by the legislative provision or regulation or decision of the National Commission for Data-processing and Civil Liberties authorizing automated processing, or by the preliminary statement made before the implementation of such processing, is punished by five years' imprisonment…".

Non-compliance with purpose is mainly due to commercial reasons. The sale of files between commercial companies, giving rise to profitable exploitation, can sometimes lead to crimes being committed. Determination also involves the right to be forgotten: processing cannot last for an indeterminate time period.

C) *A right of access is provided, usually directly*[13], *at no excessive cost*. The file controller cannot refuse access unless the request is part of a form of harassment, which has so far never been the case. If these requests are met with silence equating to a denial on behalf of the file controller, the physical

10 Directive of October 24, 1995.
11 (A) of article 2 of directive 95/46.
12 Article 226.21 of penal code.
13 The right of indirect access relates, for example, to information services, which some magistrates and the CNIL can access.

person in question can call upon the national regulatory authority on the matter of personal data, which can order the file controller to respond to the request. An explicit refusal could result in the file controller being penalized, possibly financially. If the physical person notices that some data are incorrect or incomplete, they can use their right to rectification. The rights of access and rectification are not only provided in European legislation, but also in the self-regulatory charters of certain professions and companies. Self-regulation is therefore highly compatible with the work of European lawmakers within the European Union. The person can also, in some circumstances, call on their right to opposition.

The automatic processing of data cannot go against the interests of the physical person: a decision cannot be based solely on the consideration of data, especially in the consideration of personality, professional results, credit, reliability or behavior.

D) *Furthermore, some data are "sensitive" and cannot be stored*: this is the rule, but there are exceptions.

The rule is clear and goes back to the principles discussed previously: sensitive data cannot be used in the processing of personal data if it contains information pertaining to racial or ethnic origin, gender, political opinions, religious or philosophical convictions, membership of a trade union, health or sexuality. Any form of discrimination based on one or several of these aspects is illegitimate.

There are several exceptions:

– the person in question has given their consent;

– processing would allow for the legal processes regarding labor laws to be respected;

– processing is necessary to defend key interests of the person involved or another person who is physically or legally unable to give their consent;

– processing has a purpose given by the supervisors that has been launched by individuals carrying out legal activities that are political, philosophical or religious in nature or that pertain to a trade union. Information can under no circumstance be passed on to a third party, or sold, even freely. There have been cases where political parties have

passed on information regarding some of their members: they were punished severely.

In terms of health, where there are a number of exemptions, exceptions are made in the interest of public health[14] in the interest of the patient or preventative medicine, or medical diagnoses, or the provision of care. The processing of data is done either by a health practitioner who has taken the Hippocratic Oath and is sworn to professional secrecy, or by a supervisor of medical procedures, who is obliged to maintain discretion. However, physical persons fear misuses in a domain where their intimacy is at stake and where the question is not clearly resolved.

The other exceptions are based on the freedom of expression and freedom of creation.

The freedom of expression allows press companies and journalists to store information relating to sensitive data concerning certain individuals, which can later be exploited by the journalists.

The freedom of creation allows authors to collect sensitive information with the objective of favoring originality. Thus, some research laboratories contain data that will be later used in publications and articles.

Finally, the treatment of data regarding offenses, penal conviction and security measures can only be effective if it is carried out under the control of public authorities. Importantly, an exhaustive list of penal sentencing can only exist under the strict control of a public authority.

Security is the priority. All those involved recognize that technical security is a main condition for freedom.

The processing controller applies the adequate technical and organizational measures to avoid any possible accidental destruction or loss of data, and any alterations, distribution or non-authorized access. The level of security is gauged based on the level of risk run by the processing of the data. If a subcontractor is chosen by the controller, it must provide adequate guarantees: they can only act on the commands of the processing controller.

14 Epidemiology.

All these elements are obligatory and feature in directive 95/46.

II) *A number of directives are dedicated to personal data in the sector of telecommunications*[15] *and in the sector of electronic communications*: the directive on July 12, 2002[16], which replaces the directive on December 15, 1997, and the directive on November 25, 2009 on universal service and personal data in the domain of electronic communications is pushing the law forward in terms of some aspects.

A) *The directive on December 15, 1997 integrates digital technologies with specific requirements*. Through national regulations, Member States guarantee the confidentiality of communications carried out on public networks. It is prohibited for any individual other than users to listen, intercept or store these communications without the consent of the aforementioned users. This ban does not apply to the legally authorized recording of communications.

1) *Data processed with the goal of establishing communications are erased or made anonymous as soon as the communication is over, except when clear purposes are laid out*: billing of subscribers and the commercialization of services by a provider. In any case, the handling of data is done under the authority of network providers or telecommunications services. For detailed billing, measures are taken so that the right of subscribers does not go against the right to privacy of calling users.

2) *The identification of calling lines can be problematic with regard to individual freedoms*. The calling user must be able to erase information on the identity of the calling line. If information on the identity of the calling line is provided, the subscriber being called has the right to refuse incoming calls when the calling user has removed information on the identity. The protective regime is removed when the subscriber begins to receive malevolent calls. In this case, data that allow identification of the person calling are preserved and provided by the provider.

Automatic call forwarding is a manifestation of individual freedom: the subscriber has the right to freely end automatic call forwarding from a third party to his or her terminal.

15 Directive 97/66 on December 15, 1997.
16 Directive 2002/58.

Personal data that are present in directories, printed or electronic, are limited to the identification of a single subscriber, unless the subscriber in question consents to the publishing of complementary information. A subscriber who would rather not appear in the directory has the right to not appear in it; this right is free in nature.

Unsolicited calls whose purpose is direct prospection by means of an automatic calling machine, by fax, or electronically are prohibited, unless previous consent has been given by the person in question[17]. The only exception involves merchants who have already conducted a transaction with a physical person. If the latter is no longer interested in the products and services of the merchant, they can express their opposition. Spamming is prohibited everywhere, but while the European Union has opted for prior consent, the United States prefers to use an opt out system.

B) *Important changes took place between the directive on July 12, 2002 and that on November 25, 2009*. Thus, while cookies[18] "can be a legitimate and useful tool", according to the 2002 directive, implying a right of opposition if the persons concerned did not want cookies, the directive of November 25, 2009 established prior consent for cookies. Websites attempt to bypass the requirements of this legislation by asking for the consent of users as soon as they enter the site. In this way, without prior consent the users are unable to access the site.

1) *Geo-localization involves prior consent and anonymity.*

Security in terms of electronic communications obliges operators to signal what are the risks, and to state the most recent technical possibilities, as well as the probable cost of such possibilities.

2) *For all the texts of the European Union, the exploitation of personal data relies on the principles of proportionality*

Nationwide texts

In the United States, only the Privacy Act regulates public data. In the United States, which is a lot less protective than the European Union, self-regulation dominates. However, this self-regulation is often optional in

17 Opt-in.
18 Cookies.

nature and privacy is not considered for personal data in the same way as in Europe.

All these texts have played and continue to play a leading role. Nevertheless, it was in the last quarter of the 20th Century that they prevailed the most, and this appears most notably in the domain of the interception of telecommunication and electronic communications. The necessary balance between security and privacy really does take privacy into account. This is true more or less everywhere, and particularly in Europe, because of the jurisprudence of the Council of Europe and the ECHR.

3

Telecommunication Interception

3.1. Jurisprudence of the EHCR

I) *The Klass affair*[1] played an eminent role in the manner interceptions are approached.

A) *The facts:* Gerhard Klass, Peter Lubberger, Jürgen Nussbuch, Hans-Jürgen Pohl and Dieter Selb, West German nationals, argued that article 10, paragraph 2 of the Grundgesetz and the law it engendered on August 13, 1968[2] are in opposition to the European Convention of Human Rights and Fundamental Freedoms.

They accepted that the German State had the right to such surveillance methods. They attacked the legislation as it does not force authorities to notify those concerned *a posteriori* and it does not allow for appeals against tribunals.

The 1968 law gives grounds for phone tapping and recording. Surveillance is licit only if the establishment of proof cannot be gained through any other means. Those concerned are not warned of their restrictions although the responsible authority must notify them of the restrictions as soon as it may be accomplished without compromising the aim of the interception.

1 ECHR, Klass affair and others, September 6 1978.
2 Gesetz zur Beschränkung des Briefs, Post und Fermelde Geheimisse.

Security and Privacy in the Digital Era, First Edition. Claudine Guerrier.

The plaintiffs were considered to have been the subject of phone tapping, but had no possibility of proving this. Their claim was denied, particularly by the Constitutional Federal Court, which claimed "In order to make a constitutional appeal against a law, it must be the law, and not the execution of the law, that violates a fundamental right".

The German government, for its part, upheld that the plaintiffs had no grounds for complaint: they could not claim to be victims; they sought a control of German legislation on a "purely hypothetical basis of being under surveillance".

The European Court of Human Rights is incompetent. Its role is to control the correct implementation of the convention when a plaintiff considers their rights to have been violated and could not obtain satisfaction through domestic means, and not to enter into ideological quibbling hidden behind judicial arguments.

B) *The law*: the EDHC accepts that an individual can, under certain conditions, be victim of a violation brought about by certain legislation without having to prove that specific legislation was applied in that case. There are therefore reasons to investigate, due to the contested legislation, whether the plaintiffs were victims of a violation. This jurisprudence is essential: it gives an extensive interpretation to the right of individual requests, which must not be overwritten by domestic measures[3].

Moreover, the court states that when a State establishes secret surveillance of which those concerned are unaware and which as such is unassailable, article 8[4] is at risk of being meaningless; these conversations, through telecommunication, are included in the notions of "privacy" and "correspondence". Was the interference justified as an exception? The plaintiffs considered the *powers* given to the German authorities could potentially lead to abuse and cannot constitute a legitimate defense for the defense of a democratic State. The court examined the 1968 law to determine whether it contained sufficient guarantees against abuse. After meticulous examination, the court did not perceive or recognize the danger of such abuses. Article 8 of the convention had not been violated.

3 Procedural causes.
4 Protection of private life.

II) *The Malone judgment*[5]

A) *The facts*: James Malone was accused of fencing stolen goods. His trial yielded dismissals on several points; during a subsequent trial, he was acquitted on insufficient proof.

Following his acquittal, James Malone took civil action against the Metropolitan Police Service before the Chancery Division of the High Court, as he considered the interception and recording of his telephone conversations to be illegal…, even if they were based on a warrant from the Minister of Home Affairs. He claimed that his correspondences, both by post and telephone, had been intercepted for several years. Although he did not possess proof, his belief was based on distribution issues, signs of mail being tampered with and noises on his telephone line. He believed, among other things, that his telephone line was connected to a "counting" instrument. While he was being charged, his correspondents were visited at home; James Malone did not believe this was a coincidence.

In England, the interception of telecommunications occurred for a long time due to warrants given by the minster of Home Affairs. The vice president defended the "English" system of administrative phone tapping before the Chancery Division. He insisted that there were no property rights on the text of a telephone conversation. James Malone cannot therefore pretend to have suffered any prejudice based on his property rights having been violated: phone tapping in post offices is not equivalent to trespassing.

In particular, English law does not guarantee a right to privacy, nor does it ensure the right to have phone conversations in one's own home without the intrusion of a third party. Consequently, James Malone, having exhausted all internal appeals, filed an appeal before the ECHR. Between James Malones' appeal and the EHCR's judgment…, the British government reflected upon the necessity of legislation for communication interceptions. In the January 1981 report to parliament, the Royal Commission on Criminal Procedure reviewed the possibility of a law[6]. The government did not follow

5 EHHC, Malone v. United Kingdom, August 2, 1984.
6 Report from the Royal Commission on Criminal Procedure, January 1981: "We recommend that the law must regulate police use of surveillance mechanisms".

these recommendations. It is considered that the current tapping system conformed to the basic principles of English law.

B) *The law*: the English government did not deny the reality behind James Malone's accusations. Interception is truly the interference of public authority, justified in the name of public benefit. The question must be to determine if British domestic law includes "acceptable judicial norms" and sufficient guarantees; English jurists hold fast to tradition.

The ECHR does not agree with such arguments. The Court views that English and Welsh law on the interception of communications for the needs of public authority is both unclear and inaccessible. A minimum degree of judicial protection is lacking. Interceptions are acceptable in a democratic society if they are not abused. However, in Great Britain, there exists a clear risk of abuse. The ECHR applies the same reasoning for telephone interception and counting procedures. It convicted the United Kingdom in the Malone affair for violation of article 8 of the European Convention of Human Rights and Fundamental Freedoms. The United Kingdom had to draw the necessary conclusions and adapt its law on phone tapping, according to EHCR's jurisprudence.

The Malone judgment was combined with a similar opinion expressed by Judge Perretti. He questioned the issue of a democratic society and its security needs faced with technological innovations. Judge Perretti was relatively pessimistic about the justification behind the balance of the requirements of public order and the protection of individual freedoms. He underlined the dangers for a democratic society faced with the permanent temptation of public authorities to know the *situation* of its citizens. Profiling is a harmful act that is too often committed. Interceptions are an instrument of this permanent inquest. According to Mr. Perretti, countermeasures are justified: the right to erasure of data and right to the restitutions of tapes. Individuals are threatened by a society of information: "The mission of the Council of Europe and its organs is to prevent the establishment of regimes and methods that would make 'Big Brothers' the masters of citizens' privacy". The Council of Europe acts best in this manner.

III) *France was to follow a similar path to the United Kingdom with the ECHR's judgment of Kruslin*[7] *and Huvig*[8].

The Kruslin Affair

A) *The facts*: on June 8 and 14, 1982, an investigative judge in Sait-Gaudens, presiding on the murder case of Jean Baron, a banker, issued two letters of request. In the second, he charged the commanding squadron leader of the research department of the *gendarmerie* of Toulouse to monitor Dominique Terrieux, a suspect. From June 15 to 17, the *gendarmerie* intercepts 17 communications. Jean Kruslin, then lodged with Dominique Terrieux, used his telephone, participated in a number of those communications, notably with a man called from a telephone box.

During the interview, Jean Kruslin and his interlocutor implicitly evoked another murder case, committed against Mr. Peré. On June 18, Jean Kruslin was apprehended by the *gendarmerie* and was placed in custody for the Baron case, and subsequently the Peré case. Before the Indictments Chamber of the Court of Appeal of Toulouse, Jean Kruslin asked for the cancellation of the litigation recording as it had been carried out in an unrelated context. The Chamber of Appeal rejected his request; there is nothing to prohibit attaching to one criminal proceeding elements of another proceeding as long as the connection is contradictory. In his appeal before the court of cassation, Jean Kruslin referred to article 8 of the Convention: "Interference by public authorities in private life… must use clear terms in order to notify to all, in a sufficient manner, the circumstances under which it allows public authority to operate such an infringement". The criminal court of the court of cassation rejected the complaint on July 23, 1985.

B) *The law*: once convicted, Jean Kruslin submitted an individual request before the EHCR. He argued that article 367 of the Criminal Code takes precedence on article 81 of the Criminal Procedure Code, which does not authorize phone tapping in express terms. According to the French government, there is no contradiction between article 368 of the Criminal Code and article 81 of the Criminal Procedure Code.

7 ECHR, Kruslin, April 24, 1990, Dalloz, 1990, 353, Pradel notes.
8 EHCR, Judgment of the Huvig couple, April 24, 1990.

The ECHR, on the other hand lists the measures designed by French law:

– the requirement of a decision to be made by an investigative judge, an independent magistrate;

– control by the investigative judge exercised upon judicial police officers;

– a potential control of the investigative judge by the indictment chamber, the lower courts and the court of cassation;

– the exclusion of devices and strategies that could constitute provocation.

– the obligation to take into account the defense and in particular the confidentiality of the relationship between the lawyer and the suspect or indicted person.

Nonetheless, these rules were insufficient, not fully protecting individual freedoms. The Commission named the main weaknesses as follows:

– the absence of precise and express delimitations of situations permitting the interception of telephone communication;

– the absence of a reference to the seriousness of the acts (crimes, offenses, possible sentences).

The ECHR provided further details as follows:

– the category of people who are likely to be wire-tapped was not indicated;

– no detail is offered in terms of the nature of the act, nor is the limitation or length of the interception mentioned;

– the absence of data on the establishment of summary minutes is damaging;

– the conservation, erasure or destruction of recordings in the case of dismissal was not included.

Thus, the procedure is not protective enough. “French law, written or not, does not state with enough clarity the extent and methods of the exercise of discretionary power by the relevant authorities, in a manner that would not consider the claimant to have had at least the minimum degree of protection

provided by the rule of law in a democratic society". According to the ECHR, the law must involve accessibility and precision, which was why they considered French procedures to be insufficient.

Moreover, French law did not provide an appeal body for interceptions. The ECHR convicted France in the Kruslin affair and ordered it to review its interception laws to create an appeal body that is independent from public authorities.

The Malone and Kruslin judgments fall under the same jurisprudential trend in keeping with the opinion of Judge Perretti in the Malone case.

From a slightly different perspective, during the decade when it was still possible to believe that Mr. Perretti's analysis painted an overtly pessimistic picture that was not open enough to the contribution of technology, the United States attempted to achieve the balance of maintaining public order and security with the need to provide sufficient guarantees in electronic communication to the American people. The influence of the basic principles and their amendments of the Constitution is perceptible. Since the 18th Century, there has been a difficulty in reconciling removing any of the rights that the American people are entitled to in the name of domestic or external security.

3.2. Interceptions in the United States

Telecommunication tapping is relatively frequent in the United States. It is regulated through Title 18 of the United States Code. At a federal level and at the level of the States, tribunals often allow phone tapping, pen-registers[9], trop and traces[10] to prevent criminal acts and collect evidence for crimes as well as on criminal groups. Criteria for legality are broader in the United States than they are in Europe.

I) *Communications Assistance for Law Enforcement Act*

A) *On October 25, 1994,* the Presidency ratified the Communications Assistance for Law Enforcement Act (CALEA[11]) also known as the law on

9 An identification mechanism for a number dialed.
10 An identification mechanism for an incoming number.
11 Public law, 103 414 47 USC 1001-1010.

digital telephony. The CALEA was to handle the rapid changes in telecommunication technology and affirm the obligation of operators to offer assistance to authorized services in carrying out interceptions of communications and identify calls.

B) So that the qualified bodies may, despite the fragmentation of the networks, be able to carry out surveillance; the CALEA demanded that all operators[12] be in a capacity to deliver a quota of requisitions by no later than October 25, 1998. The CALEA did not impose a particular arrangement or configuration on the systems. On the other hand, the government and industrialists were required to provide their cooperation to ensure the application of the measures.

The Attorney General proceeded to an estimation of the number of electronic surveillance devices and communication interceptions. This estimation established two levels of capacity, the first being the actual capacity[13], which corresponds to the quantity of communication surveillance devices that governmental agencies authorized to use such means could simultaneously use. The second was the maximum capacity[14]. Three area categories were defined; categories I and II encompass areas with high electronic surveillance activities. Only a few highly populated areas in the United States fell into category I. Densely populated areas and suburbs mostly fell into category II. Category III was composed of all other geographical areas. Areas served by an operator fell at the least under category III, if not II or I.

The CALEA was accused of concealing essential information such as the definition of operational cooperation and stating the basis upon which projections used to record the needs of the services that carried out the law were completed.

The Minister of Justice delegated responsibility for the implementation and administration of the CALEA to the Federal Bureau of Investigations (FBI). Congress authorized in section 109 the allocation of 5,000 million

12 Section 103 of the law.
13 CALEA's actual capacity: for category I, 0.5% of the operational capacity of equipment capable of emitting or receiving communications; for category II, it is 0.25%; and 0.05% for category III.
14 CALEA's maximum capacity.

dollars during the fiscal years of 1995 and 1998 to support the expenditure generated by modifications on equipment and installations in order to obtain necessary capacity. Section 109 also allowed for the offset of expenditure incurred by ensuring the compliance of equipment and installations, in the instance where the federal commission was to ascertain that the requirements of capacity, the requirement of capacity were not met. The FBI created parameters to determine the amount of money likely to be paid by the government.

In the fiscal years of 1995 and 1996, no steps were taken in the implementation of the CALEA. A proposition for the allocation of funds was discussed, and then adopted in the summer of 1996 by the Chamber of Representatives and by thy Ministry of Justice in 1997. On April 11, 1996, the FBI's first annual report on the application of the CALEA was published and presented to Congress. For decades, security interceptions have had a legal basis in presidential orders or federal regulations. From 1975, the regulatory zeal increased[15].

II) *Foreign Intelligence Surveillance Act*

The Foreign Intelligence Surveillance Act (FISA) was adopted in 1978.

A) *FISA only permits telecommunication interceptions on electronic, mechanical or other types of devices*[16]. The reason is described in generic terms: "Information concerning foreign intelligence activities", which is necessary to protect the United States. The reasons are as follows:

– possible or proven attacks, sabotage (an infringement of Article 105, Chapter 18 of the United States Code);

– international terrorism;

– clandestine activities that could harm the United States and benefit foreign intelligence services.

15 Namely, executive order no. 12036 on January 24, 1978, replaced by executive order 12333 on December 4, 1981 (Federal Register, vol. 46, no. 235, p. 59941); executive order 12334 on December 4, 1981 (Federal Register, vol. 46, p. 596), the creation of the *President's Intelligence Oversight Board.*

16 FISA's Article 101(f) no. 1.

The terms are general and at times insufficiently precise. They leave a margin of interpretation and evaluation open to security officials.

A distinction is established between American citizens and foreigners residing on American territory. A foreign national is considered the agent of a foreign country if they may engage in intelligence activities. An American citizen will only be considered an agent of a foreign country if they knowingly perform intelligence activities[17,18].

International terrorism has been the subject of comprehensive analyses and evaluations. It incorporates the following:

– violent acts that physically place a person in danger and that violate not only American criminal law but also foreign laws;

– acts of intimidation that are aimed at threatening the government or civilians by murder, kidnapping and diversion; these provisions are equally applicable outside U.S. territory[19].

B) *Authorization requests are developed by federal agents*, who address a surveillance request to the competent judge[20]. The request has no legal foundation if it does not receive the agreement of the Attorney General, whose role is to examine the requests in accordance to their legal grounds[21]; the request is accompanied by detailed information on the following:

– the identity of the agent;

– the power of attorney received by the President of the USA's Attorney General in order to grant such authorizations;

– the Attorney General's agreement;

– the identity (if known) of the person that will be intercepted or (if unknown) a description of those placed under surveillance;

– a summary of the facts that appear to justify the request for interception;

17 Material elements: intelligence activities; moral element: malicious intent.
18 Article 101(b), FISA.
19 Article 101(c), FISA.
20 Article 103, FISA.
21 Article 104(a), FISA.

– a presentation of the planned use of computer files (indication of the procedure);

– a description of the necessary information to be assembled and the nature of the communications to be assembled;

– a guarantee given by the representative of the President of the United States for national security (or by a high-ranking delegated official from National Security or Defense that the President will have chosen through the recommendation and with the approval of the Senate) based on objective criteria.

The monitoring is done for the benefit of a foreign power[22]; the only goal of the operation is to obtain this intelligence; the request is submitted because all other types of usual enquiry are unsuitable or unreliable; a description of the means used, a declaration relevant to prior requests concerning the persons, equipment, locations and length planned for the surveillance.

The agents that submit the request guarantee the truth of their statements or declarations are under oath[23]. The legal requirements for requests are numerous: they prevent abuses and excesses that could limit freedoms.

In practice, the administrative burden and the management costs incurred by processing them have led judges to accept standard formulas. By saving time and money, is there not a risk of removing the initial intention of preserving individual freedoms? It is indeed a possibility. Courts of competent jurisdiction[24] have been invited to demonstrate vigilance so that formalism does not cancel out explanatory statements. Nonetheless, the procedure is simplified when the representatives of foreign countries are subjected to surveillance or interception.

While authorization requests are submitted for approval to the Attorney General, it is the judges that issue orders. The judges are FISA court magistrates. Orders are unilateral (ex-parte order), without a hearing before

22 Article 101(e), FISA.
23 President Clinton decided that only the director of the FBI had the right to sign. If unable to, the director of the CIA could stand in for him.
24 FISA Court.

the tribunal of the concerned party. The principle of contradiction cannot be justified in a field where secrecy is so important.

The usual duration for such authorization shall not exceed three months although it is renewable[25]. Exceptions are made for foreign agents (private persons), or for foreign legal entities; the length can reach a year.

In case of an emergency, the Attorney General can make orders with the approval of a judge; he must give 24 h notice to FISA's court of competent jurisdiction and a request for regulation is then submitted.

The orders state that the telecommunication operators[26] and the proprietor or landlord must assist the service that made the request for information. Private persons who offer assistance toward the surveillance or interception measures have an obligation of confidentiality that is applicable in all countries in terms of surveillance or other security interceptions.

The U.S. government provides compensation to private persons. The hindrance caused by counter-intelligence and security measures should be limited. Individuals working for intelligence services who provide assistance are compensated.

There currently exists in the United States a certain balance, which is still under re-evaluation, between security needs and the needs of individual freedoms.

3.3. European states and interceptions

I) *The United Kingdom*

A) Following the Malone judgment, *the 1985 law "The Interception of Communication Act"* grants the Minister of Home Affairs (due to previous practices) the responsibility of issuing interception authorizations. In the case of an emergency, a high-ranking official may give orders for an interception as long as the situation is regularized in the following 48 hr.

25 Article 105(d), FISA.
26 Specified communication or other common carrier.

There are a few reasons, as follows:

– national security[27];

– the prevention or discovery of a serious crime[28];

– safeguarding economic prosperity.

Being aware of market conditions, the United Kingdom is conscious of the risks toward financial actors and industrials caused by the efficiency of economic espionage (illicit transfer of knowledge and information from one company to another). These patterns can only be invoked if the information cannot be acquired by means more respectful of individual freedoms. The duration of the security interception is of 2 months, renewable for another 6 months if national security is threatened. The minister can cancel the authorization if it is no longer considered necessary.

The notion of quotas appears to be a foreign concept. In reality, three factors limit the annual number of telephone conversation interceptions: technical capacity needed to execute the interceptions, the reluctance to surpass budget and a willingness to manage costs as well as a governmental desire to concentrate on priority targets without diluting its vigilance.

Execution requires cooperation between competent authorities that issue authorizations and the telecommunication operators. The operator deals with the monitored line and must record all intercepted conversations. He/she provides the equipment and ensures its functioning and transmits the recorded tapes to the service that requested the interception. Operations are authorized by a senior police or customs officer.

Jurisprudence adjudicates on the contested point of the legality of obtaining proof through public or private means. Prior to August 1984, British Telecommunications was “in charge of public telecommunication services”. This monopoly was abolished by Article 2 of the 1984 law, which

27 According to the report from the Commissioner for National Security: terrorism, espionage, subversive activities that place public security and property in danger and that aim to suppress parliamentary democracy through violence (N 27. 31).

28 According to the report from the Commissioner (1986): serious crimes are those that are violent, aim to achieve significant material gain and include a certain number of participants that have the same objective, and for which a perpetrator who has no judicial priors may incur a prison sentence of at least 3 years (N 25).

came into force on August 5, 1984. Provision of telecommunication services was regulated by Part II of the 1984 law.

Article 5 of the 1984 law states that no person may operate a telecommunication service in the United Kingdom without it having been permitted by a license. Article 8 states that certain persons, notably British Telecommunications, could be granted licenses containing special provisions that would impose the provision of telecommunication services.

B) *The 1984 law was analyzed* with regard to the 1985 law on interceptions of postal communications or communications through public telecommunication systems. Without a warrant issued by the Minister of Domestic Affairs, the intentional interception of communication during its transmission is considered illegal. Persons believing to have had their communications intercepted may request an investigation before a special court[29].

Article 9, paragraph 10, refers to persons who could conduct interceptions[30]. Article 10 attributes "public telecommunication system" the same definition as the law of 1984. Jurisprudence adjudicated on public systems in the Effik[31] and Ahmed[32] judgments.

If the Court considers that the complaint is valid and the interception activities were unconstitutional, it will notify the complainant,[33] submit a report to the prime minister and make an ordinance that serves as a basis for the following:

– declaring the illegal interception to be null and void;

– ordering the destruction of documents, not merely the originals but all copies and duplicates;

– engaging the executive to pay for damages incurred to the complainant.

29 Article 7, Paragraph 2.
30 "All persons concerned with paragraph 2 are: all of the Crown's civil servants, all postal workers, all public telecommunication operators, and all those implicated in the operation of a public telecommunication service".
31 R v Effik and others, July 1994.
32 R v Ahmed, March 29, 1994, non.pub. until Effik affair.
33 A rare occurrence.

If the court does not believe there to have been an interception or if it is convinced of the legality of a current interception, it will inform the individual that their rights have not been infringed. The individual is not notified *a posteriori* of surveillance activities of which they are subjected.

The Ministry of Domestic Affairs has mediatized this appeal; flyers that included claim forms have been placed in postal and telecommunication offices.

II) *Germany*

A) *The legislation for interceptions in the Federal Republic of Germany has existed since August 13, 1968*. The G10 law has long proven to be reliable. The reasons and competent authorities for interceptions are stated.

The reasons are as follows:

– prevention or repression of threats to democratic or liberal order[34];

– protection of the existence or security of the Federation and the Land;

– defense of national security and public order as well the prevention of criminal offences;

– prevention of threats against the security of NATO troops.

B) The measures of interception are only legal if all other methods are destined to fail or cannot yield a tangible result. The authorities that were likely to request communication interceptions in 1968 were as follows:

– BFV, the Federal Office for the Protection of the Constitution;

– BND, the Federal Intelligence Service;

– LFV, the State Office for the Protection of the Constitution;

– MAD, the Military Counter-Intelligence Service.

It was members of the executive that could permit the authorization of interceptions: the supreme authority in the land for the LFV, the ministers for Justice and Domestic Affairs in other cases and a commission[35]

34 West Germany was supposed to be a democratic reference as opposed to East Germany, in the context of the Cold War.
35 Article 9, Paragraph 4.

composed of three members and three deputy members who were elected by a college who in turn was voted for by the Bundestag. The members' term coincided with that of the Bundestag and as such expired following the election of a new Parliament. The opposition was also represented in this commission, having access to all documents. The elected college was constituted of five Bundestag deputies that were regularly informed of the correct application of the G10 by federal minsters. This college then held elections for commission members and approved the designations of critical and dangerous areas.

C) *Authorization must be made in the written form*. It is then transmitted to the service that requested it and to the telecommunications operator. Article 1, paragraph 4, allows a maximum of 4 months of interception, renewal is possible.

The wiretapped individuals can be warned in certain cases; interception measures are notified to concerned persons if the notification does not compromise the end goal of the interception.

A new law was adopted during the second semester of 1997. It placed greater emphasis on security, allowing judges and German police officers to proceed to interceptions of conversations at a distance and wiretaps in private housing in police inquiries when particularly serious offences were involved.

Members of professions subject to professional secrecy can be intercepted, although members of the clergy and criminal lawyers are excluded[36]. Furthermore, parliamentarians by virtue of possessing elected legitimacy are equally excluded.

Authorization is provided by a commission comprising three magistrates. In the case of an emergency, authorization can be given by only one of them. It is issued for a duration of 4 weeks, but it is renewable. If the intercepted person is subject to professional secrecy, the use of gathered information must involve another authorization. These particular cases are reported by the government to Parliament every year. The text was contested as being in contradiction to article 13 of the Grundgesetz. As such, the Constitution was

36 In order to preserve defense rights.

modified in January 1988 in order for the security changes to come into force.

III) *Austria*

Austrian legislation is considerably different to that of its German neighbor, which is explained by their differing histories.

A) *Until 1997, legal interceptions were issued by a judge*, and in cases of emergency by the prosecution. Authorizations could be issued for crimes or offences possessing a sentence greater than a year. As such, the cut-off was relatively low and the field of application relatively wide. Persons likely to be intercepted were suspects and third parties related to the suspects.

B) *Austrian law no. 105, published on August 19, 1997, is precise*. It allows wire-tapping and video surveillance of suspects during police inquiries. These are equally authorized for cases of abduction and confinement of persons as well as permitting the elucidation and prevention of crimes that could entail over 10 years in prison. Surveillance is similarly permitted for the elucidation of delinquencies that can entail a sentence of over a year's imprisonment.

The decision to grant authorization is made by the investigative judge or by the Ratskammer upon request from a public prosecutor.

The recordings are then subjected to a review; police services or the investigative judge will file a comprehensive report on the methods used at the end the surveillance period. The prosecutor may have access to the visual or sound recordings, which are kept accessible for consultation.

Austrian legislation is less protective than German legislation, which has long sought to be a "window" of democracy.

IV) *Italy*

Legal interceptions are only possible as exceptions. They are ordered by a judge, and in emergency situations by the Prosecutor for a limited list of offences incurring a minimum of a 5-year sentence (lower limit for individual freedoms). The duration of the interception is of 15 days, although it may be renewed. All recordings must be fully transcribed. However, mafia interceptions are relatively high.

V) *Switzerland*

Legal interceptions are possible when ordered by a judge, and, in case of an emergency and serious offences by the prosecution. The order lasts for 6 months and can be renewed. Recordings that are not essential to ascertain the truth are kept separately and destroyed at the end of the procedure.

In Switzerland, certain cantons allow for the possibility of appeal against unjustified wire-tapping. In some cases, the court of cassation can adjudicate a request for compensation. The 1992 report to the Federal Council concerning telephone surveillance suggested that once the interceptions were complete, the concerned individual could take legal steps to have the legality of the procedure examined and could be awarded reparation. On February 17, 1993, the Federal Council decided it would be injudicious to provide reparations.

VI) *Belgium*

In 1990, Belgium was an unusual example in the legality of interceptions as it enshrined the principle of the inviolability of telephone communications. An exception existed nonetheless; instead of a "legal interception" there was a "telephone communication tracking". The investigating magistrate could thus procure an authorization for a criminal investigation.

On June 30, 1994, the law on "wire-tapping, monitory and recording of private communications" was adopted. It sought to include all lessons in jurisprudence from the European Court of Human Rights. Interceptions are judicial. They are permitted "in order to protect the people against terrorism and serious crimes". The investigating judge or the Royal Prosecutor[37] (in cases of obvious offence such as hostage situations or blackmailing) authorizes the interception. For serious crimes, terrorism and organized crime, it is the investigating judge who intervenes.

Authorization is given for 3 months, and this cannot be renewed for more than 6 months. If a lawyer or doctor is concerned, the investigating judge must notify the President of the Bar or Medical Association.

37 In the instance of the Royal Prosecutor, an investigative judge must confirm the measure within 24 h.

VII) *Spain*

Secrecy of communication is guaranteed by the Constitution[38]: "Secrecy of communications is guaranteed, particularly regarding postal, telegraphic, and telephonic communications". The same article gives the basis for legal interceptions as it notes the exception "in the event of a court order". The order is issued by a judge for 3 months, which can be renewed several times.

Article 55[39] of the constitution states that the secrecy of communications can be suspended in a state of emergency or siege (martial law) due to an organic act that is aimed at the investigations of activities of armed bands or terrorist groups. The organic act on December 1, 1980 is an antiterrorism arsenal. It authorizes the suspension of part of or all fundamental freedoms (inviolability of the home, communications secrecy, right to freedom and security) for certain category of people due to their adherence to incriminated groups or their alleged participation in delinquent or criminal activities.

The reasons given are misdemeanors (or crimes) against a person's physical integrity, illegal detention and ransom, possession of arms, munitions, explosives and breach of external State security; these offences are considered as "terrorism" by the Spanish Criminal Code[40].

Authorization for the interception of telephone communications has to be granted in writing by the competent legal authority. In case of an emergency, it may be granted by the Minister of Domestic Affairs, the director of State Security: the judge is informed and must delay or confirm the decision in a maximum of 72 h. Authorization is given for duration of 3 months and is renewable. The concerned people are not notified if such a notification could harm the proper functioning of the State, although criminal liability and compensation exists in case of abuse.

After decades of dictatorship, Spain became a democracy[41], although there remains a difficulty in reconciling the requirements of freedom with security measures.

38 Article 18, Paragraph 3.
39 Paragraphs 1 and 2 of the constitution.
40 Many misdemeanors were in the name of independence.
41 For further information, see [HER 97].

In January 1996, a Spanish judge leading an inquiry into communication interceptions by intelligence services issued a dismissal: the tapping was used in the defense of the State.

VIII) *France*

A) *The Schmelk Commission*

Before France's conviction by the ECHR, the Schmelk commission, a commission of parliamentary inquiry that operated without hindrance from military secrecy under the Mauroy government, examined the state of interception laws in France and issued propositions for reform.

The Schmelk Commission's propositions tended to conserve the existing legal framework as far as it was compatible with the general principles of law.

Security interceptions would be exceptional. The Commission proposed the following reasons: seeking intelligence concerning France's security, prevention of breaches to State security, prevention of breaches to public security and prevention of organized crime.

The execution of these interceptions would be limited; intelligence that possessed no relation to the legal reasons must be reduced or suppressed; documents must be destroyed as soon as they are no longer necessary.

A law would serve as a legal basis for security interceptions. Debate was provoked within the Commission as to whether authorization should be granted by a magistrate from the judiciary or from a governmental authority.

Some members of the commission agreed with the magistrate of solution 3, as it would entail that all interceptions fell under the mandate of the judiciary. However, the majority of the members of the Commission were favorable to a governmental authorization. The institution of a judge would upset the existing structure. Furthermore, security interceptions were primarily the concern of the executive. The issue of emergency was difficult to reconcile with a prior authorization issued by a judge. These suggestions

provided reference despite the fact that the Schmelk report did not have an immediate impact and was not published straight away.

B) *The law of July 10, 1991*[42]

After the ECHR's conviction of France, and the injunction to reform the methods of interception on French soil, French law is based on both the recommendations of the ECHR as well as the Schmelk Commission's recommendations. Thus, on July 10, 1991, a new law was adopted and was applicable until 2015, dealing with both legal interceptions and security interceptions.

1) *Legal interceptions* are authorized for investigations (in 1991, there were no interceptions at the enquiry stage, this was to be initiated by the law on March 9, 2004) by the investigative judge when the sentence is at least 2 years' imprisonment. French law does not detail a list of crimes and offenses. Legal interceptions have a duration of 4 months and are renewable. They are transcribed and are only destroyed at the expiration of public action, even if the case is dismissed or acquitted.

Exceptions are few and far between, and rarely involve parliamentarians. There are no protected professions. Even lawyers, who carry out the right of defense, can be intercepted in their homes or offices if presumed to be an accomplice to their client. Under these circumstances however, the President of the Bar Association is notified. There are no real statistics on legal interceptions with lawyers, although they do appear to be numerous despite protests from lawyers and certain legal experts.

2) *Security interceptions*

They can occur if they conform to six reasons, as follows:

– National security: this covers national defense as well as other breaches to the security and authority of the State.

– Prevention of terrorism: while this allowed for consensus, some parliamentarians wished to delve further into incriminations and not merely prevention. However, France had been the victim of multiple attacks during

42 Law 91-647.

that period, and as such the necessity in preventing organized assassinations for political reasons was imperative.

– Prevention of organized crime and delinquency: this incorporates illicit narcotic trafficking, organized crime networks, the trafficking of arms, munitions, explosives and nuclear material, counterfeiting, serious financial crime, human trafficking and art theft.

– The reconstitution or maintenance of dissolved groups: the defense of public freedoms at the expense of threatening small groups seems to justify this reason.

– The protection of France's fundamental scientific and economic interests: this is a new reason. Fiscal wiretapping was evoked during a debate at the National Assembly. The Minister of Justice sought to be reassuring: security interceptions cannot be used during fiscal enquiries and for customs matters they are limited to combatting drug trafficking and money laundering from said trafficking. Could this be harmful to banking secrecy? Nearly all transfers between banks are done through computer systems and the stock exchange in Paris operates in a similar manner.

– Authorization requests are centralized within ministries: the Ministers for Defense, the Interior, and in charge of customs are the only ones authorized to make requests from their services, particularly intelligence services, to the Prime Minister.

The Prime Minister has the sole right to authorize security interceptions. He acts as a guarantor but also as a policy maker: as head of the administration, he cannot be issued with an injunction. The Prime Minister is assisted by his delegate, as he cannot commit actual time to examine the files. Authorizations are issued for a duration of 4 months, are renewable and do not involve offences; this is why recordings and transcripts are destroyed so rapidly in less than 10 days.

The work is primarily carried out by the GIC[43]. In 1991, they only carried out a part of the interceptions in Paris, as they possess an important division in Lyon as well as in multiple other provincial zones.

43 "Groupement interministériel de contrôle": inter-ministry control groupings.

A maximal number of interceptions are likely to be authorized by the prime minister.

3.4. Interception controls

I) *The USA*

A) *FISA and computer data*

FISA includes provisions to prohibit measures[44] that use computer data incorrectly. These measures, however, are not detailed. Nonetheless, the law lists procedures that could be stopped by the Attorney General.

B) *Controls*

I) *FISA considered the possibility of a request refusal and methods of appeal*. If a request is at first refused in court, it is possible to take the request to another court having three judges appointed by the President of the Supreme Court among judges from Courts of Appeal or District Courts[45]. The President of the Supreme Court equally appoints the presiding judge for the Court formed for this occasion. A judge in the FISA Court is appointed for 7 years with an annual renewal. Re-election is prohibited[46]. The District Court's decision is applicable to all federal and State courts except for Appeal Courts. The District Court's decision can be reviewed before the Appeal Courts and the Supreme Court.

If the findings occurred on American soil by use of devices whose surveillance purposes fall under FISA's definition, information can be destroyed if the Attorney General considers that the content may be harmful to an individual. Intelligence obtained through the FISA system are shrouded in secrecy and not exploited when it comes to American citizens. In terms of criminal matters, this intelligence can be used with the consent of the Attorney General and the person and their lawyer are notified. The person in question can then have recourse to the territorially competent lower federal court and to invoke the inadmissibility of the "evidence" collected through these specific means; they may attempt to demonstrate that the evidence

44 AM 101(h), FISA.
45 Courts of Appeals.
46 Article 103, FISA.

was not collected legally and that surveillance was not in agreement with the law.

2) *There is also a public control.*

The Attorney General, the primary person responsible for authorization measures, must (due to the nature of his office) submit an annual report[47] to the administration of the Federal Courts and to Congress on the application of FISA. The report namely mentions the total number of requests and renewals, specifying how many requests have been denied. Studying these reports allowed us to find out the tendency toward increasing numbers of requests without a single refusal. Only a single request had been modified by a FISA court.

As the Courts' archives cannot be consulted, it is impossible to determine whether judges are scrupulously respecting the letter and the spirit of FISA or if they are prioritizing a security interpretation of the law.

Every semester, the Attorney General informs Congress Select Committees[48] on surveillance activities[49]. The Committees, of which there are two, have the right to assemble other intelligence insofar as they are necessary to the correct completion of their mandate. The Parliamentary Committees state the application of the law once their chambers are assembled. These reports occasionally include observations and propositions.

In the United States, a person subjected to these measures is not informed of them. On the other hand, the concept of "protected persons" is well entrenched and taken into consideration for certain professional secrets.

Intercepted conversations cannot involve lawyers or priests. It is important to keep in mind the highly valued status of lawyers as well the protected status of religion in the United States. Article 110 of FISA states that all persons having suffered prejudice due to a surveillance measure or due to an indiscretion caused by these measures has the right to official

47 Article 107, FISA.
48 Select Committees on Intelligence.
49 Article 108 (a), FISA.

compensation. The FBI must cease interceptions as soon as a protected person intervenes.

In terms of sentences, FISA can give out fines of 10,000 dollars or more and a maximum 5 years prison sentence.

II) *Controls in the United Kingdom*

There exists two types of controls; one by the Commission and one by a tribunal.

A) *The Commissioner*

The Prime Minister appoints[50] a person in charge of controlling whether the executive's exercise of power is in compliance with the law. This person is the Commissioner, and is endowed with in-depth legal expertise. He is given legal functions and receives payment included in the Parliament's budget. All agents partaking in interception aid the work of the Commissioner by providing him with the documents and information that he needs. The enquiry is precise: if it reveals illegal actions, the government commissary writes up a report and sends it to the Prime Minister.

The president also establishes an annual general report on the conclusions drawn on the confrontation between the law and its application. The report states the number of authorized interceptions, which can be several hundreds. It is presented to the House of Commons and the House of Lords. The Prime Minister can prevent the publication of certain passages destined for Parliament if he considers the incriminating paragraphs could threaten national security, prevent crime or safeguard the British economy. Relative transparency is desirable, but cannot threaten security.

Due to the reports being written by judges, they contain judicial concepts and interpretations. Commissioners have elaborated jurisprudence.

B) *Control by tribunal*

Another form of control is performed by the Interception of Communication Tribunal, of which all members possess a legal background and at least 10 years' experience. The members of the tribunal are appointed

50 Paragraph 88 of the Interception of Communication Act.

by the Queen – that is to say by the Prime Minister. They belong to the parliamentary majority and their impartiality is assured.

Individuals believing to be the subject of interception may take their case to the tribunal. The claim is followed by an inquiry, and the tribunal is assisted by the commissioner, who possesses all elements necessary to the clarification of the tribunal. If the tribunal considers that the claim is valid, that an unconstitutional interception has occurred, then the claimant is notified[51] and a report is submitted to the Prime Minister that promulgates an order that:

– declares the invalidity of the illegal interception;

– orders the destruction of all documents, not simply the originals but all copies and duplicates;

– engages the executive to pay damages incurred to the claimant.

If the tribunal does not believe there to have been an interception or if it is convinced of the legality of a current interception, it will inform the individual that their rights have not been infringed upon. The individual is not notified *a posteriori* of surveillance activities of which they are subjected.

The Ministry of Domestic Affairs mediatized this process appeal; flyers that include claim forms have been placed in postal and telecommunication offices.

The situation has since evolved. On July 2, 1996, the House of Lords rejected Mr. Khan's appeal against the judgment of May 1994 by the English Court of Appeal. The rejection of the appeal had motives: it did not want to adjudicate upon the admissibility of a criminal trial in which evidence had been collected by wire-tapping allegedly installed in a manner that would be considered trespassing and property damage. Indeed, the argument is based on Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. The Convention is different from English domestic order. According to English law, the police acted in good faith and the irregularities did not make the case inequitable.

51 A rare occurrence.

At the end of 1996, a bill was presented. It was linked both to the police and to interceptions in "The Interception of Communication Act". It stated: "No introduction or interference in a property or telegraphy is illegal" if the chief constable deemed it necessary.

It was rejected in the House of Lords and provoked much controversy[52]. In August 1996, the Minister for Domestic Affairs published a code of conduct in which he explained the precise circumstances in which police and custom officials may penetrate by the use of interception into a private home, office and hotel room in order to collect information that may be used to prevent or repress criminal activities. Confidential information acquired by doctors, lawyers, journalists and the clergy can thus also be collected. Operations are authorized by high-ranking customs or police officers and a control is carried out by the Commissioner.

III) *Controls in Germany*

It is worth noting that when East and West Germany were reunified, it was West German law that was adopted for the newly reunified country.

A) *Parliamentary controls*

Relevant ministers are subject to controls by submitting to parliamentary control. The PKK/4 and the commission for parliamentary controls of federal intelligence services do not control the application of the G10, but ministers must inform the college composed of Bundestag deputies.

B) *The constitutional court of Karlsruhe*

Any German citizen who considers their fundamental rights to have been denied can issue an application to the constitutional court. The constitutional court has accepted appeals even when not all legal avenues had been exhausted.

C) *Sentences*

The G10 law does not list sentences related to authorized interceptions. The German Criminal Code[53] stipulates imprisonment or fines for unauthorized interception measures. Article 3, Paragraph 3 of the law on the

52 52 J.R Spencer "Bugging and burglary the police", The Cambridge Law Journal, January 31, 1997.
53 Article 201 of German Criminal Code.

cooperation between the Federation and the Länder states that this text is applicable to intelligence agents.

IV) *France*

A) *A control body was created for security interceptions at the request of the ECHR*. The National Commission for the Control of Security Interceptions (CNCIS) is an independent administrative authority similar to the CNIL, but does not possess an advisory power toward the Prime Minister. The CNCIS includes a President who acts as a guarantor of public freedoms and institutions, appointed by the President of the Republic. The first President was Paul Bochet, a jurist specialized in human rights cases. He gave a certain legitimacy to the CNCIS. His successors have had different profiles, all being State advisors with undeniable legal expertise in administrative law, although they have given a somewhat technocratic character to the position.

The other two members of the college are a deputy, appointed by the President of the National Assembly, and a senator, appointed by the President of the Senate. One of these two parliamentarians must belong to the opposition in compliance with a commitment made before the ECHR, although this was not included in the July 10, 1991 law.

B) *The college has a variety of tasks*: controlling the compliance of purposes, controlling the execution of the interceptions, referral by individuals.

Its first task, the control of authorizations, which is the determination of whether authorizations comply with their purposes, justifies the existence of the CNCIS even if it does not result in sanctions. This control takes place upstream and prior to the issuing of the authorization, with exceptions made for emergencies or extreme emergencies. Subsequently, all notices are given upstream. The prime minister can overturn a notice, although this rarely occurs.

Equally, the CNCIS carries out controls on the execution of interceptions and can discontinue decisions if it appears that certain practices deviate from the letter and spirit of the 1991 law[54].

54 This is extremely rare.

The CNCIS plays a role for appeals from individuals in keeping with the wishes of the ECHR.

Certain individuals may believe they are subject to an interception. Faced with uncertainty, they may submit a claim before the CNCIS so that it may be verified. Those concerned most certainly hope for an answer that they will not necessarily receive. The commission must proceed in the same manner as if they had generated the claim themselves and notify that the work is being carried out[55]. It cannot operate otherwise, an administrative authority must respond to mail, notably claims.

This does not entail that the individual will be satisfied. A private individual, even if familiar with the law, becomes involved with a control body hoping that the procedure will allow them to determine whether their "imagined" interception did indeed take place.

Legislators are not preoccupied with "fantasies". They must be as precise as possible. If a violation is detected by the CNCIS, they refer to the public prosecutor.

Furthermore, the CNCIS writes an annual report that is submitted to the prime minister, as well as the Presidents of the National Assembly and the Senate. It is accompanied by a covering letter that summarizes the main points and conveys the general tone of the collected data and impressions. Each word is carefully reviewed by the CNCIS' modest team. The report includes comparative law studies. It is particularly exemplary in terms of statistics as it shows not only the distribution of interceptions by purpose, but also the number of security interceptions. The number of legal interceptions is often tainted with journalistic exaggeration, but the number of security interceptions is reliable. Once published, the report is often consulted by lawyers interested in interceptions.

A comparison between the varying references is necessary. Two contradictory tendencies are noteworthy as follows:

– the first is manifested as a strengthening of individual freedoms as desired by the ECHR. The freedoms are the gauge of the democratic character of the nation state;

55 Article 17 of the July 10, 1991 law: "When the commission has exercised its control following a claim, it is notified to the author of the claim that the necessary procedures are underway".

– the second is reminiscent of the security discourse. Maintaining public order appears more challenging than in the 1980s.

Lawyers have slowly begun to identify the concepts of legality and lawfulness. It is important, however, in order to reach a balance between the maintenance of public order and the preservation of individual freedom to conceive of laws that take into account the requirements of freedom, as advocated by the ECHR's jurisprudence, and the maintenance of public order as influenced by each country's different histories.

Interception laws have more or less managed to maintain this balance. On the other hand, it is evident that the aforementioned balance is desirable for Western democratic States and an effort in legal securing has been obtained to link the two main variables: public order and freedoms with an emphasis placed on the cultural traditions of each country.

4

Biometrics and Videosurveillance

In this era, other methods of control seek to link security and freedoms.

4.1. Biometrics

Biometrics, which is based on the use of personal data, must follow principles of proportionality. This is why it is possible, in some cases, for legal persons to refer to fingerprint recognition, or genetic fingerprints, and in other cases, other biometric methods can be required.

I) *France*

A) *In this country, operation is controlled by the National Commission for Informatics and Freedoms – the CNIL.*

1) *The CNIL allows fingerprints to be used when the safety of individuals is at risk: the principle of proportionality is applied.*

a) *Some sites store dangerous materials.*

For example, the CNIL approved a request made by the La Hague site of the company COGEMA (*Compagnie Générale des matières nucléaires*) to install fingerprint readers for use by staff and visitors. The storage of nuclear material is not without risk: some zones are classed top-secret. In this case, the creation of a fingerprint database is justified.

Security and Privacy in the Digital Era, First Edition. Claudine Guerrier.

b) *The purpose of security, with regard to individuals, can also be applied to airports*.

This can also be applied to some flights. With permission from the CNIL, Air France has tested a biometric technique that uses fingerprints at the beginning of flights going to Tel-Aviv, Israel. The objective is to verify whether the person boarding the plane is the same person who registered the bags at check-in. Fingerprints are recorded using an electronic reader at the check-in desk, and then compared with results from a similar reader upon boarding the plane. Despite giving permission for the operation to take place, the CNIL has required that the confidentiality of information be respected.

c) *This proportionality is also applied in some areas of airports*.

In Roissy and Orly, trials have been conducted around the control of "reserved security zones": this affects the access of the staff of *Aéroports de Paris*, public services and companies operating within the so-called "reserved security zones". The CNIL reacted positively to this trial[1]. The safety requirements respect the principle of proportionality, but the end purposes should not be misappropriated. In France, fingerprints are used for these experiments. The lessons learned from the airports at Roissy and Orly are very informative, as much for companies and developers, who would like to use biometrics, as for the CNIL, for whom the use of biometrics must remain exceptional. Experiments are generalized and apply to individuals entering these "reserved security zones" of the airports of Orly and Roissy. The proposal to have biometric templates on individual access cards has started to be implemented.

d) *The principle of proportionality also involves public services*.

In this way, proportionality has been applied, partially, in the case of the *Académie de Lille*, to ensure the safety and proper running of *concours* (exams). The *Académie de Lille* had provided the CNIL with a request concerning the access of the personnel of the *Education Nationale* into academic areas. They proposed a system of access based on fingerprints, without controlling the duration of access of the personnel. Personnel representatives were informed about the project: the personnel, in its

1 Deliberation 02-034 on April 23, 2002.

entirety, were provided with information regarding the project; according to the secretary general of the *Académie*, the project received no objections. The CNIL established two purposes: the first corresponded to the identification of the personnel permitted to enter the academic areas. The second purpose focused on the safety of the exams and the *concours*[2], which are organized within the *Académie*, and on the status of the personnel able to access the buildings with regard to the organization of the surveillance of the exams and the *concours.*

According to the CNIL, according to the principle of proportionality the purpose does not justify the creation of a fingerprint database. The second purpose, on the other hand, warrants the creation of a fingerprint database, on the condition that the areas in question be identified[3]. The database is made up of three modules, the "person" module with the names, surnames and usernames that allow access to other modules, the "right of access" module with the authorization profiles of the individuals, and the "fingerprints" module with templates of the fingerprints.

e) *Proportionality is also found in the preservation of culture*: cultural heritage needs to be protected and preserved – for reasons different from those of airports, certainly, but just as valid. Works of art have high financial value, as well as cultural value, and in museums they are exposed to the public.

In this context, in 2001 the Louvre museum requested permission to use biometric processes to ensure the security of the goods stored in the museum and to control the working hours of the subcontracted employees involved in cleaning and maintenance.

The Louvre museum has created out-sourced contracts, based on a certain number of hours worked, a sign of the evolution of the public market.

2 Confidentiality of exams.

3 "Analysis of the file allowed determination that such was the case for the exam printing plant, the vaults and archive rooms containing personnel files. As a result the commission limited fingerprint recognition and the subsequent database to these areas and to the personnel permitted to access them, and has taken steps to ensure the confidentiality of this data"; 21st activity report of the CNIL, p 116, La Documentation française, 2001.

This public market is built around specific arrangements, which are explained by the quality of the works on display in the Louvre museum: employees of subcontracting companies are submitted to an approvals procedure: bulletin two of the criminal record is examined. The use of biometrics would ensure that only approved agents have access to the Louvre museum. However, the biometric method chosen is not fingerprints, but palmar recognition, which is far less intrusive than fingerprints, and has not been associated with traceability.

Information concerning the approved agents of subcontracting companies is stored as long as the employee is employed by the company providing the service. Data regarding hours of work are stored digitally for a period of 1 year. This storage is explained by the need for companies to preserve information on the hours worked by employees over the year in case it is required by work inspectors. The CNIL expressed its approval in this case because the duration of the conservation did not seem excessive with regard to the purpose of increased security. Employees have a right of access and rectification.

2) *Genetic files are also based on the principle of proportionality*: in France, DNA can be used for the FNAEG (*fichier national automatisé des empreintes génétiques*) automated DNA database. This database[4] aims to prevent crime by allowing the DNA of potentially dangerous criminals to be stored. This takes place in the context of international cooperation on the matter of criminal policing: the results of DNA analysis identification coming from abroad can be stored in the database.

Data can be erased following a request from the *Procureur de la République* or following a request made by the party concerned. A competent magistrate must make his or her decision known within a period of 3 months. Following an absence of response, or if the magistrate does not order erasure, the party concerned calls upon the liberties and detention judge.

Recorded information can be preserved for up to 40 years, starting from the request for recording, or from the day of definitive sentencing.

4 The FNAEG was created through law 98-468 on June 17, 1998.

3) *The principle of proportionality aims to protect individual freedoms*: biometric processes cannot be used if the end purpose does not justify it.

B) *When the purpose is not related to security, regulatory authorities can express their reservations*

1) *The purpose can correspond to a control of access. School canteens are the source of much debate in Europe*. The Collège Jean Rostand in Nice had chosen a biometric database revolving around the automatic recognition of the fingerprints of the physical persons involved. This involved associating a coded representation of the fingerprints of pupils and personnel members with administrative and management information. This project was approved by the parents of the pupils and representatives of the personnel.

However, the CNIL expressed its fear that a fingerprint database could potentially be used for purposes other than the one expressed: they filed a negative response, citing the disproportionality between the method and the desired objective[5].

On the back of the lessons learned during the Jean Rostand project, Carqueiranne Collège has proposed a system of control based not on fingerprints but on a technique using hand outlines. The CNIL approved this: changes of the end purpose seemed impossible[6].

On the contrary, two Catholic establishments found themselves in a situation of illegality. Since 1999, access to the canteen of l'Immaculée Conception, a Catholic education establishment going from preschool to high school, has been controlled by a biometric fingerprint recognition system. To eat, the children and teenagers have to put their thumb onto the scanner[7].

5 "While the creation of a biometric database, including fingerprints, can be justified in certain circumstances where the security and identification requirements are compelling, its presence in a high school, containing information regarding minors, with the sole objective of controlling access to a school canteen, is excessive with regard to the purpose in mind", Deliberation no. 006015 on March 21, 2000.

6 "The hand outline technique used by the Collège de Carqueiranne, unlike the fingerprint system used in the Collège de Nice, has no impact in everyday life, and therefore allows for no possible misuse", CNIL press release, October 15, 2002.

7 "This allows us to ensure the children are indeed at the canteen, which is an obligation of ours with regard to the parents. Depending on the number of times the child has used the service, we can then produce a bill for the parents" stated the treasurer.

Jeanne d'Arc Collège, for its part, has introduced a system based on fingerprints to control access to the canteen.

The schools have initiated no request procedures with the CNIL; these are therefore illegal situations.

A comparison can be made with what is happening in the United Kingdom.

In the United Kingdom, the Venerable Bede School in Sunderland[8], established in September 2002, has decided to install an iris recognition biometric system to control the pupils' access to the canteen.

By the start of the 21st Century, 400 British schools were already using infrastructure installed by the Scottish company CRB Solutions and the automatic admissions program called Impact. This system involves the use of a magnetic card that parents load up at the counter or online, which relieves the pupils of the need to carry money, as well as reducing queues.

At Venerable Bede, CRB Solutions has added the biometric recognition system set up by the American company Iridian Technologies – a specialist in iris recognition – to the system Impact.

The choice was made to use the iris rather than fingerprints for reasons of efficiency[9]. Palmar recognition has not been considered.

In this set-up, before sitting at their table, the pupils must be identified by a video camera. This analyzes the image of the outline of their iris and conducts a comparison with the templates stored in the school database.

The regulatory body on the matter of personal data protection in the United Kingdom has not expressed itself yet. The high school has given its reasons for the rather large investment, stating the need to accelerate the process and its desire to avoid loss of canteen cards. On the other hand, human rights associations are fighting against the measure, considering it a violation of privacy and individual freedoms. One of these is Privacy

8 Near Newcastle.

9 "… finger morphology changes considerably in adolescents, while the outline of the iris remains identical from a very young age" David Swanston, director of CRB Solutions.

International, which is claiming a PR stunt is behind this: "This really is like taking a sledgehammer to crack a nut. For a high school, the use of magnetic cards is largely sufficient. This type of initiative is a complete PR stunt…Personally, I find this inappropriate, degrading for the child and dangerous for the future", declared Simon Davies, at the time president of Privacy International.

2) *The principle of proportionality has also been put to the test in monitoring working hours*. An employer has a right to monitor the number of hours worked by their employees. Cybersurveillance, whose possible misuses have been flagged by the CNIL[10], and biometrics are both methods that an employee can use to monitor the activities of their employees[11].

There is a temptation for companies to use biometrics to control hours. Well aware of this need, some biometric companies are offering a "working hours management" option.

In the last 20 years, the obligation to be present at a place of work, whether administrative or a company, has involved identification. The presentation of an ID badge is anonymous. This is why the use of biometric processes has been considered.

For this reason, the prefecture of Hérault made a request to the CNIL relating to the installation of an automatic data processing system of nominative information allowing for the identification of agents working for the prefecture. The goal was to manage hours worked and establish flexible working times using fingerprints. This system would overcome the shortcomings of a badge system. This involves presentation of the badge upon entry into the prefecture, after which the agent in possession of the badge places one of their fingers onto the fingerprint reader. The identification process is reliable: it helps avoid fraud. The CNIL weighed up

10 Report on cybersurveillance, CNIL, 2001.

11 "The veil present between the CEO's office and the employee's workplace used to be opaque. New technologies make it clearer every day. First came the foreman, followed by the access card, telephones and switchboards, and itemized bills. Today, we can also add the Internet, instant messaging, biometrics, cryptography, electronic signatures, certification and perhaps ones day individual control by intradermal chips, without mentioning the potentials present in genetic engineering" in "Cybersurveillance des salariés et règles de preuve devant les Prud'hommes" by Geneviève Folzer and Mathieu Abbous, Strasbourg, January 17, 2003.

the advantages and disadvantages of such a system. The advantages included staff morale and an increase in security in a building affected by the *Plan Vigipirate*. Staff representatives were invited to a presentation by the provider. According to the prefecture, the overall impression was favorable. Regarding the increase in security, this is more debatable as the use of badges seemed to fulfill all the security criteria of the *Plan Vigipirate* in all buildings involved. The disadvantage lies mainly in the disproportionality between the purpose of working hour monitoring and the creation of a fingerprint database, which could potentially be misused to the detriment of the members of staff: "Such an objective does not seem to justify the creation of a database of the fingerprints of the personnel working at a prefecture. Furthermore, this process as a whole seems neither adapted nor proportional to the goal pursued"[12]. This verdict was accepted by the Hérault prefecture.

With the same justification,[13] this time not in the public sector but the private one, an airline company submitted a request to the CNIL for automatic processing using fingerprint reading. The process was based on two biometric clocks that identify employees using their fingerprints: these would be used to record the amount of time worked. The CNIL judged that there was lack of proportionality between the end purpose and the dangers invoked by the creation of fingerprint database. Prison personnel have expressed their opposition to extending the use of biometrics, normally limited to the movement of inmates, to monitoring work hours. Notably, the General Union of Prison Guards at Fleury-Mérogis has expressed its strong opposition to biometric targeting.

At Hyères hospital, management had wanted to submit staff to fingerprint monitoring to verify work hours. The CNIL returned an unfavorable verdict.

During its plenary session on April 8, 2005, the CNIL confirmed its previous reservations regarding the use of biometric systems in workplaces.

Within companies, the debate is not yet over. Most employers are favorable to the use of biometric systems to control the working hours of

12 CNIL deliberation no. 00-057 on November 16, 2000.
13 At Roissy Charles de Gaulle.

their employees. The most commonly used processes are palmar and iris recognition. Fingerprints are the most controversial in this debate.

On the other hand, regulatory organisms on the matter of personal data protection and employee trade union representatives are opposed to the biometric monitoring of working hours.

The situation is liable to change. If one of the involved parties changes their stance, biometrics could very well start to be used to control working hours. While the technology allows it, legal security is not in favor.

C) *Freedom of movement and biometrics*

1) *Freedom of movement is a human right*, but States, and some regional areas are liable to impose limits on this freedom. A legal balance has been sought in this matter for the right to asylum and immigration.

The right to asylum has led to several legal measures being introduced at the level of the European Union.

The Dublin Convention[14], to which all Member States adhere, and which became applicable starting in 1997, deals with asylum seekers and the control of asylum applications. It looks to avoid illegal aliens entering European Union territory. Due to possible fraud, the ministers in charge of immigration have established a text that aims to compare the fingerprints of asylum seekers.

2) *With entry into force of the Treaty of Amsterdam*, a new legal basis for asylum policy has been developed. This is the regulation of December 11, 2000, adopted by the Council and the Parliament. The regulation allows the fingerprints of asylum seekers to be stored. In Parliament, the debate was rather heated. In two rulings on 7 July and 21 September, 2000, the Parliament had ruled against the recording of the fingerprints of minors. The Council later overrode this. The data recorded are the fingerprints, the State where the asylum seeker comes from, gender and reference number. They are kept for 10 years and encrypted. The use, transmission and erasure of the

14 Convention on June 15, 1990, completed through regulation no. 343/2003 of the Council on February 18, 2003.

data follow directive 95/46. The Commission carefully monitors the security of the data. It informs the Parliament and the Council of any measures that it undertakes. Any asylum seeker subject to prejudice due to a bad application can obtain compensation. The State in question is exempt – partially or completely – of its responsibility if it can show that it was not involved in the event leading to the damage. A monitoring authority is created: it is made up of two representatives of the regulatory bodies of each Member State.

Another piece of regulation[15] surrounding the application of the preceding regulation is adopted by the Council and the Parliament: it highlights certain characteristics of Eurodac.

3) *Eurodac* came into force on January 15, 2003. It contains a central identification system for the fingerprints of asylum seekers, and, in 16 European countries, it also contains an electronic transmission system for the fingerprints with the goal of combatting illegal immigration. With Eurodac, Member States can identify asylum seekers and individuals illegally crossing a Union border. After analysis of the fingerprints, States are able to know whether an asylum seeker or an illegal alien has already made a request in another State of the European Union. The end purpose is to combat multiple asylum requests.

The central fingerprint matching system, the AFIS[16], is managed by the European Commission. The digital database, the methods of secured electronic transmission between States and the central database are what constitute Eurodac. The central system determines the techniques required for the transmission of fingerprints electronically. If technical problems arise, it can call on other methods. The reference number links the fingerprint to the physical person, and identifies the Member State that sent the data.

Eurodac was first tested in the *United Kingdom*. Political asylum seekers trialed cards with a chip containing their fingerprints, provided by the Home Office. An Application Registration Card[17] is given to the asylum seeker; it contains the fingerprints, a photo, the family name, date of birth and

15 Regulation 407/2002.
16 Automated Fingerprint Identification System.
17 Application Registration Card.

nationality of origin. It replaces the form previously provided on paper, which was too easily tampered with.

Before the creation of Eurodac, it was nearly impossible to know if an asylum seeker had previously made a similar request in another signatory State of the Dublin Convention. For the Convention to be applicable, a system needed to be in place that allowed each Member State to control whether an asylum seeker had previously made a request in a State linked to the Dublin Convention.

The measures, since the adoption of the Eurodac regulations, are applicable to all persons over the age of 14, as the opposition of the European Parliament regarding minors was not upheld.

They concern States of the European Union as well as three other countries who have introduced Eurodac in their territory: Norway, Iceland and Switzerland. As a result, through fingerprints, biometrics has become widespread for asylum seekers.

Switzerland, for example, introduced FIT in October 2002 in its 26 cantonal police forces, linked to the central system in Bonn. With AFIS, FIT is a technical solution that allows each State to connect with Eurodac. It benefits from compatibility with international standards[18]. It was first introduced in Norway and has been in use for over 10 years in Scandinavia. Moreover, the NAP[19] is safely moving communications onto the Testa network. FIT has also been used in the context of the Schengen Agreements for the exchange of information over the SIRENE network. It allows police forces to share fingerprints and photographs digitally to help with the identification of wanted individuals.

Eurodac respects directive 95/46 on the protection of personal data. The use of fingerprints is nevertheless controversial.

II) *The USA*

A) *From 1993 onward, American authorities in charge of immigration installed a system named FAST*[20] *in New York airports*. This system allowed

18 Notably Interpol and the FBI.
19 National Access Point.
20 Future automated screening for travellers.

for the identification of passengers. It followed on from Project INPASS[21]. The goal was to improve passenger care. Willing passengers would give their identity and a template of the palm of their hand during check-in. If palmar recognition could not be used, fingerprints were used. The template was recorded onto a card, the content of which was updated each year. The passengers involved in the program were, for the most part, Canadian or American, and, to a lesser extent, nationals of other States, signatory of visa-waiver agreements. INPASS was also a response to identity fraud.

B) *Biometrics has been used extensively in the control of migration*. In 1940, a law was passed aiming to regulate the influx of aliens onto American soil. This law stated that all foreign entrants into the United States had to register their fingerprints. Two sets of these had to be taken, one for the consul and the other for the American authorities, who would transfer the file to the immigration services for examination, and then onto the Attorney General. Minors under the age of 14 were exempt from this process. The Illegal Immigration Reform and the Immigrant Responsibility Act of 1996 generalized the procedure through the introduction of an automatic control system for entry and exit in and out of American territory, with the goal of detecting individuals staying beyond their prescribed duration.

The Immigration and Nationality Act applies the procedure set out in the Alien Registration Act of 1940 on foreigners over the age of 14 staying in the United States for more than 30 days. All individuals must submit a fingerprint template in order to obtain a visa. Section 326 of the law encourages the Immigration and Naturalization Service to develop a system of identification for foreign criminals in order to stop their entry onto American soil and to help with police searches. This uses facial recognition technology.

The system in place before the Patriot Act would go on to demonstrate the effectiveness of biometrics, as well as its shortcomings in terms of personal freedoms following the attacks on September 11, 2001.

4.2. Videosurveillance

Videosurveillance originated in Nazi Germany, but it really rose to prominence in the 1950s, especially in the United Kingdom from 1953

21 Immigration and naturalization service passenger accelerated service system.

onward. The United Kingdom is the European country that started using videosurveillance the earliest. The first CCTV cameras were installed in 1953, for the crowning of Elizabeth II, becoming increasingly widespread in the 1990s, particularly from 1994 onward. Also very early, the Information Commission Office, which is the regulatory body for the protection of personal data, focused on possible videosurveillance misuses.

I) *The United Kingdom*

The Information Commissioner's Office (ICO) details the process of surveillance consisting of four phases: the first phase, videosurveillance, has a public and precise end purpose. The second step is the "routine", and the third is "systematization". The fourth step is that of selective videosurveillance: videosurveillance aims to cross-reference information, classify it and share it. The ICO has found that errors are relatively numerous. Two thousand seven hundred cases of identification mistakes were recorded for the registration plate recognition system[22]. Generalized surveillance is considered a discriminatory violation of the right to free movement in the United Kingdom. Since 2001, the daily life of individuals with non-UK origins has become considerably more complicated and slowed. This is the result of an increased number of stops for these groups than for others.

From the start of the 21st Century, Richard Thomas, President of the ICO, has condemned abuses of videosurveillance. He stated that the United Kingdom would "sleepwalk into a surveillance society". The development of videosurveillance results in a significant reduction in the freedom of movement, and increases distrust in civil society. According to Richard Thomas: "surveillance feeds suspicion: employers who install such devices in their workplaces do not trust their employees. Parents who use webcams and GPS to watch their children are also admitting a lack of trust". For Richard Thomas, this equates to social suicide. Children tend to internalize the outlines of such a surveillance society and limitations to the freedom of movement. The ICO is very pessimistic.

II) *France*

France was later to install CCTV and seeks to find a balance between security and freedoms. Legal precautions must be taken.

22 Registration plates are one of the simplest examples.

In 1993, two senators, Françoise Séligman[23] and Alfred Dreyfus-Schmidt[24] initiated the drafting of a law on the use of videosurveillance for roads and public places[25]. The draft suggested that the installation of cameras on roads should only take place after approval by the CNIL; in the case of a denial, installation could only go ahead following a discussion by the municipal council, approved by a decree from the State Council. Although the proposal was rejected, this time period was marked by deliberations regarding the role of the CNIL and videosurveillance. Louise Cadoux presented a report to the CNIL called "Vidéosurveillance et protection de la vie privée et des libertés fondamentales" ("Videosurveillance and the protection of privacy and fundamental freedoms")[26]. Following three favorable judgments regarding the establishment of videosurveillance systems, with digitization and recording of images and sound, it became necessary to determine whether digitization consisted of a nominative form of data processing, and whether the CNIL was competent in the domain of videosurveillance[27]. CNIL policy was moving toward this. Louise Cadoux focused on the shortcomings of the law on July 17, 1970 on image rights, and maintained that the CNIL was competent on the matter of videosurveillance in public and private spaces. She considered the recorded images to be a collection of photographs likely to contain faces identifiable using other files, and as such to be a non-automatic file of nominative data. In his DESS thesis on videosurveillance[28], David Forest states: *"*for a society having produced a color image from a photograph to keep this image on a computer, without keeping any information relating to the person photographed, it cannot be considered to be a nominative for of data processing as defined by the law of January 6th 1978 (…)". In this way, the court refused to consider that an image alone could constitute nominative data, excluding images from the field of application of the law on January 6, 1978. On the other hand, Louise Cadoux considers that the photograph of a

23 Then Senator for Hauts-de Seine.
24 Senator of the Belfort territory.
25 Proposal submitted on May 18, 1993, but not on the agenda.
26 Louise Cadoux, "Vidéosurveillance et protection de la vie privée et des libertés fondamentales", report of November 30, 1993 presented to the CNIL.
27 Sylvie Rozenfeld, "Vidéosurveillance : la CNIL s'interroge sur sa compétence", in *Expertises des SI*, January 1993.
28 Juriscom.net, June 20, 2000 mentions the decision of the first room of the tribunal of first instance of Paris. Judgment of 22 March, 1989.

person is "potentially nominative information", as it can easily be reconstituted in three dimensions, or cross-referenced with a name directory.

This position would come up again in the CNIL deliberation on June 21, 1994[29]: "Images of individuals must be treated as nominative information allowing the identification of these individuals, at least indirectly by comparison with other criteria". However, nominative data are information that, directly or indirectly, can lead to the identification of physical person.

According to Eric Heilman and André Vitalis[30], an image is a privileged factor for identification. In her report, Louise Cadoux remarks: "no piece of information is better for revealing the 'racial origins' of a person, or even their religious convictions, than an image, none more so than a photo"[31]. Sensitive data are nominative data.

A) *The law on January 21, 1996*, the first big law on videosurveillance in France, did not share this line of argument, and referred judgment to the Tribunal of first instance of Paris[32].

In his report on the law project on orientation and programming relating to security, meaning to integrating specific arrangements legalizing videosurveillance in public areas and areas open to the public, Senator Paul Masson[33] listed several arguments for the CNIL's incompetence on the matter of videosurveillance, notably focusing on a lack of material means and an excessive workload. However, suggestions made during the CNIL deliberation on June 21, 1994 were repeated, but with one important change: the ban on visualizing the entrances and the inside of public areas has turned into a ban on recording the entrances and insides of residential buildings. Deputy Gérard Léonard[34] argued that banning the recording of the entrances

29 Deliberation 94-056 of June 21, 1994 adopting a recommendation on the methods of videosurveillance installed in public areas and those open to the public.
30 Eric Heilman, André Vitalis, "La vidéosurveillance: un moyen de contrôle à surveiller", in *Le courrier du CNRS*, no. 82, May 1996, p 48.
31 Meaning "sensitive data" in the sense laid out in directive 95/46.
32 Anne-Cécile Lorant, "La vidéosurveillance et la loi du 21 janvier 1995", in *Droit de l'Informatique et des Télécoms*, no. 4, 1995, p 12.
33 Spokesman for the draft law in the Senate.
34 Spokesman for the draft law in the Assemblée nationale.

of residential buildings is unrealistic. Freedom of movement is at stake here: how can one film "a street and its sidewalks without the camera encompassing the doors of residential buildings? If the monitoring of entrances and exits of buildings are to be avoided, it is better to avoid videosurveillance in public areas altogether".

After claims of non-compliance with the constitution made by the socialist group, the Constitutional Council is faced with making a distinction between two criteria of equal legal value: the exercise of public freedoms, including the freedom of movement, and the prevention of attacks on public order. The plaintiffs relied on three arguments: the law does not follow the principle of proportionality of police action, the law does not provide enough measures guaranteeing the exercise of fundamental freedoms, including the freedom of movement, and the law referred points touching on fundamental aspects of public freedoms to implementation decrees. They did not mention the competence of the CNIL. On January 18, 1995, the Constitutional Council decided that the proposer of the law had successfully combined public order and the respect of public and individual freedoms[35]. A single passage on the erasure of recordings targets the law on January 6, 1978. The debate on the competence of the CNIL did not take place during the adoption of the 1995 law. It did take place, however, in later years, at a national and community level.

According to recital 16 of directive 95/46, "the processing of data made up of sound and images, such as those used in videosurveillance, is not included in the field of application of the current directive if they are used for reasons of safety, defense, State security for the exercise of State activities pertaining to the domain of penal law or for the exercise of activities that are not included in the field of community law".

The law on January 21, 1995 has a bigger scope of application than directive 95/46. The automatic processing of images and sounds recorded using videosurveillance materials are included in the field of application of the directive and the law on January 6, 1978.

35 Sylvie Rozenfeld, "La vidéosurveillance est constitutionnelle", in *Expertises des SI*, January 1995, and Nguyen Van Tuong, "La décision du Conseil constitutionnel du 18 janvier 1995 sur la loi d'orientation et de programmation relative à la sécurité" in *Les petites affiches*, no. 48, April 21, 1995, p 18.

In 1996, the CNIL published a new report by Louse Cadoux[36], dealing with the transferring of "letters and numbers to voice and image". Images of a person, like their face, belong to the category of information that can result in the identification of physical persons. Louise Cadoux establishes a non-limiting list of image recognition techniques, from 3D cameras to editing software using insertion, mixing and face-altering techniques.

André Vitalis states the concept of information is not accurate and problematic in terms of data protection: "a digital replica, previously exclusively made of text, thanks to images, and soon, sound, becomes multimedia resource that does not have the same ramifications as textual data".

The nominative data debated during the adoption of the law on January 21, 1995 was not changed by the following laws, notably the law pertaining to the rights of citizens in their relations with administration, which states in article 8 that the law on July 17, 1978 would be changed, with the deletion of the notion of nominative documents.

Deputy Claudine Ledoux instigated a report[37] that pointed out the contradictions and difficulties in defining nominative data between article 4 of the law on January 6, 1978 and the provisions of article 1 of the law on July 17, 1978 authorizing the communication of non-nominative data to third parties.

According to jurisprudence from CADA[38] and the State Council, the nominative character of a document does not come from the existence of identifying elements, but from information on the physical person, or descriptions of their behavior. However, the notion of a "nominative document" is likely to be misleading as it implies the person has been named. In any case, the concept of nominative files has long been required in declaring a videosurveillance system in French law.

36 "Voix, image et protection des données personnelles", La Documentation française, Paris, 1996.
37 Report made in the name of the commission for constitutional laws, legislation and general administration of the Republic, on the draft law adopted by the Senate on the rights of citizens in their relations with the administration, no. 1613, May 19, 1999.
38 Commission for the access to administrative documents.

On top of a declaration made to the CNIL, in France videosurveillance systems also require authorization from the geographically relevant prefect (in Paris, this is the police prefect), as well as a notice from the departmental commission for videosurveillance[39].

B) *The departmental commission for videosurveillance* consists of five members: the president, who is a magistrate of the judiciary, chosen by the president of the appeals court; a magistrate of the administrative jurisdiction, who is a member of the order of administrative tribunals and the administration appeals courts; a mayor, chosen by the departmental mayoral associations; a representative chosen by the chamber(s) of commerce and territorially competent industry; a person chosen for their competence by the prefect. The mandate is of 3 years. It can be renewed once.

The departmental commission instructs the application for authorization of videosurveillance systems, with the exception of systems relation to National Defense. It can require a hearing with the applicant, additional information, and the advice of any person qualified or involved in the application. It gives its opinion to the prefect, who is not obliged to follow it, and who can grant a request despite opposition from the commission. Moreover, this opinion is not made public: members of the commission adhere to a policy of professional secrecy, meaning they do share all or part of the decision, and do not discuss the information that was involved in the process.

The commission is a regulatory body. The law on January 21, 1995 states: “any individual involved can refer to commission regarding any problems stemming from the operation of a videosurveillance system. The provisions laid out in the previous paragraph shall not interfere with the right of the person involved to refer to the competent jurisdiction, if need be in the form of an emergency procedure”.

The commission is competent on the matter of the access to images. In the context of the right of image, any person whose image has been recorded by a videosurveillance system has the right to request access to this image. The person responsible must follow through, but can refuse the request in the name of public security and national defense. The commission is then

39 Decree no. 96-926 on October 17, 1996.

referred to, but they cannot force the person responsible to change their decision.

The process of notifying the commission can also relate to the operation of the system itself, and notably the erasure of images. These must be destroyed within 1 month at the most: these are included in the rights of physical persons. The right to act is open to any person who can justify a direct interest. The person must first have contacted the individual responsible for the videosurveillance system directly and have not obtained a satisfactory response to their enquiry.

Notification of the commission does not automatically lead to legal action. On the contrary, if legal action does take place, the commission avoids adjudication to avoid the risk of contradiction between any jurisdictional decisions on the one hand, and the reasoning developed by the commission on the other hand.

The commission does not have the ability to refer cases to itself regarding the operating conditions of a videosurveillance system, and it cannot go ahead with investigations on its own; however, it can delegate to one of its members the task of collecting useful information relating to a request of which it has been notified[40].

The law does not actually provide the commission with any objectives of control. Incidentally, the commission is not competent on disputes over the existence of a system or the validity of an established authorization: this hypothesis was removed by the Parliament to avoid pitting the commission against a prefect who delivers the authorizations, and to avoid confusion between the different legal courses since challenging an authorization involves administration jurisdiction and appeals concerning misuse of authority.

Therefore, the commission does have a regulatory role, but rather a consultative one, and is therefore limited.

The technologies used for interceptions, biometrics and videosurveillance, while already enabling surveillance and control today, still fit into the balance required by the European Convention for the

40 Article 15 of the Decree on October 17, 1996.

Protection of Human Rights and Fundamental Freedoms between public order and security on the one hand, and the preservation – even relative – of privacy and individual and collective freedoms on the other hand.

This balance involves democracies that are Members of the Council of Europe, but also all other Western powers, including countries geographically more distant from our field of study, such as Australia and Japan. These States are members of a Western block, formed from work done after the Second World War on the matter of human rights. These rights, or even "human rightsism", are heavily involved in the Western ideology that has been the base of military alliance pacts. Indeed, up to the dissolution of the Warsaw Pact, the latter was in opposition with NATO, not so much in Europe where peace was ensured by this very bipolarity, but in areas of conflict, notably the Middle East.

With the end of the Warsaw Pact, the end of the so-called socialist States ("State capitalists" would probably be more suited), and the rise of liberalism, a new layout appeared, with a single military alliance, NATO, and the pre-eminence of the United States, as much economically as strategically.

At the same time, Russia became a member of the Council of Europe, and the old members of the Warsaw Pact applied to join the European Union.

Moreover, the developing countries represented in the The United Nations conference on Trade and Development (UNCTAD) were not able to achieve a balance between western powers and other countries. These developing countries used interception systems, and sometimes biometric methods and videosurveillance, but far less than Western States with high Gross domestic products (GDPs).

This era corresponded in part to an apparent victory of democracy within States, regions and multinational zones.

PART 2

The Era of Surveillance and Control

From the beginning of the 21st Century onward, the technologies and services used by these technologies have grown exponentially. Clearly, this refers to informatics, which has flooded the globalized world market, as well as other technologies involving different aspects of human knowledge and science, as much in the area of communications as environmental, biotechnology and anotechnology.

This technology has the potential to monitor and control everything. As described in "The Prince" by Machiavelli, States have always been attracted to notions of control and surveillance. This is also true for the most prominent agents involved in Economics and Finance. In the 21st Century, as part of a globalized economy, where some countries are emerging from their relative underdevelopment and are starting to contribute to the development of multilateralism, States must deal with the myth of Big Brother. We shall explain how they have fallen for the myth, at least partially.

The technologies most likely to contribute to the takeoff of informatics and communications have, and are, experienced great successes. They increase the temptation for States and interlinked multinational companies, in multimedia and the Internet, to exert control over civil society, in the name of security for public collectivities, and in the name of profit for multinational companies.

Security and Privacy in the Digital Era, First Edition. Claudine Guerrier.

Furthermore, geographic strategy is undergoing new development. The United States is the only pre-eminent superpower in the unipolar world of today, and is conducting military operation after military operation in various areas. Other States are not able to compete with the United States, even those also on the Security Council of the UN. Russia has not yet recovered from the end of the bipolar world and the Warsaw Pact, a time where it was one of the two major powers. Emerging economic powers, China and India most importantly, despite major investment in the aviation and maritime industries, cannot rival American omnipotence and its system of alliances, NATO, of which the old countries of Western and Central Europe are members.

The United Kingdom remains the favored ally of the United States, having intervened together in Iraq and Afghanistan. France, which is a member of NATO, had preserved its diplomatic and military independence since leaving the military bodies of NATO in 1966. However, it is growing increasingly close to the United States, has rejoined these bodies and is now a considerable contributor, notably in Africa. The United States is therefore in a capacity to impose its military-industrial complex and its doctrine of national sovereignty.

Technologies relating to information and communications, nanotechnology and the technologies involved in environmental industries and services fit perfectly in this unipolar and single-centered world, where they take up a role of mass surveillance and monitoring.

5

The Sources of Law in the Field of Security Illustrate This Change

5.1. The USA

I) *The Patriot Act*

A) *The Patriot Act was passed following the attacks on September 11, 2001*; being highly mediatized, in the eyes of patriotic Americans and their allies, these attacks seemed to "legitimize" the use of new methods of control that had little regard for individual freedoms.

The Patriot Act of United States was adopted by Congress unanimously minus one abstention and signed by President George W. Bush[1]. The usual distinction between inquiries carried out by external intelligence services and federal agencies in charge of criminal inquiries[2] disappears when agents are accused of terrorism.

B) *This lengthy law permits interceptions without prior authorization*, without the use of Foreign Intelligence Surveillance Act (FISA) courts. The interceptions are increasing both on American soil and externally under the supervision of the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI). In the first few years following the Patriot Act, few

1 October 26, 2001.
2 FBI.

Security and Privacy in the Digital Era, First Edition. Claudine Guerrier.

complaints are filed before the State courts, and human rights movements, usually so vigilant, are silent.

Sixteen provisions of the law have come into force for 4 years. Amendments were made to laws on immigration, banking transactions and FISA[3]. According to Section 403, Paragraph C of the Patriot Act, the Departments of Justice and State must, with the support of the National Institute of Standards and Technology, develop technologies used to identify visa applicants and persons entering the American territory. The chosen technology is identical in all administrations in order to facilitate exchanges. Federal administrations dealing with immigration are encouraged to implement the best procedures to control immigration and ensure border security. Section 405 stipulates that the Attorney General submit a report to Congress on the FBI's fingerprint databases. This report also reviews systems used in other federal administrations. According to Section 414 of the Patriot Act, identification mechanisms are set up not only in airports, but also in nautical ports and all ports of entry to the American territory.

Furthermore, the Patriot Act recommends the use of biometric techniques and other means that make it possible to identity documents to be unfalsifiable. A biometric passport authenticates the identity of citizens travelling abroad. The document is highly secure, although extremely costly. It contains an integrated circuit in which the image of the holder and biographical information are inscribed. Foreign countries also contribute toward the costs: countries participating in the U.S. Visa Waiver Program must install machines capable of reading passports. The Pentagon, for its part, employs the "Terrorist Information Awareness[4] Program" in order to fight terrorism, which includes the installation of a database that records medical and financial data as well as information on presumed terrorists. Congress brings program specifications to the Pentagon[5].

C) *Title V, called the "Removal of impediments to the investigation of terrorism", reformed the FISA of 1978* by facilitating the cooperation

3 Law on the surveillance of foreign intelligence.
4 TIA.
5 http://www.aclu.org.

between intelligence agencies responsible for external security and agencies in charge of internal/domestic security[6]. It grants the FBI a wide authorization over National Security Letters (NSLs) that are issued directly by the FBI without any kind of judicial review, which forces legal entities under private law, particularly Internet service provider (ISPs), to communicate access to their personal database to the FBI. Thus, the use of NSLs has led to the surveillance of many American citizens who have not been suspected of terrorist activities. Currently, section 505 of the Patriot Act forbids the ISP and other legal entities to reveal the transmission of personal information to the "targeted" persons. At the end of 2003, the Attorney General authorized agencies to retain data collected through the intermediary of NSLs, if it had previously been destroyed due to it concerning people whose innocence had since been established. He gave the order to record these data on processing systems for data mining, and Executive Order 13388[7] expands the access to these databases to local governments. In January 2004, the FBI initiated the Investigative Data Warehouse in order to better manage these data. The ministerial instructions from the Attorney General allowed the FBI to integrate data originating from LexisNexis and CoicePoint by combining personal data from the public sector and the private sector.

D) *Jurisprudence*: in 2004, the American civil Liberties Union (ACLU), which had started to emerge from its lethargy, engaged in an appeal[8].

Doe vs. Holder led to an amendment to the law following the decision by Judge Victor Marrero in 2007, as this measure violates the First Amendment of the Constitution as well as the principle of the separation of powers. Despite this appeal, the modified measures were once again judged unconstitutional in December 2008.

In September 2006, a court in the Library Connection vs. Gonzales judged that accompanying NSLs with a gag order was, in the case of the Library, unconstitutional. The FBI had demanded of a library employee in Connecticut that he provide all information which he was able to access.

6 Section 504.
7 Further Strengthening the Sharing of Terrorism Information to Protect Americans.
8 Doe v. Holder.

Internet Archive vs. Mukasey, which had employed the diligence of the ACLU and the Electronic Frontier Foundation, both civil parties, resulted in a mutual agreement: the FBI withdrew its NSL demand in April 2008.

Other ACLU requests[9] resulted in the following conclusions: the Department of Defense had abused its use of NSLs and had cooperated with the FBI in order to circumvent the law.

On July 21, 2005, however, the House of Representatives approved the prolongation of the application of the Patriot Act's provisions. Among the 16 provisions of the Patriot Act due to expire on December 31, 2005, 14 were made permanent.

The two other provisions, relating to telephone interceptions and to the access to personal files, were extended for 10 years, whereas amendments were adopted to bring "guarantees" to the application of the law. The revised text was adopted in 2006.

It contains measures that aim to restrict the use of article 215, which grants the FBI and other intelligence agencies or agencies that maintain order the ability to search companies, medical cabinets, teaching establishments, book stores and libraries when the apprehended documents may have a link to the ongoing investigation. It also concerns NSLs and the exploitation of personal data, as well as telephone interceptions.

The Senate approved the extension of the law on March 2, 2006, while the House of Representatives approved it on March 7, 2006[10].

On March 9, 2007, the Department of Justice announced that the Patriot Act had been used illegally by the FBI in order to secretly obtain American citizen's personal information.

On August 17, 2006, American Federal Judge Anna Diggs Taylor declared telephone interceptions as set out by the Patriot Act to be

9 Based on the FOIA.

10 On May 26, 2011, the Patriot Act was renewed by Congress until June 2015 after voting in the Senate (7 against 23), and in the House of Representatives (250 against 153).

unconstitutional and ordered the termination of the internal surveillance program expedited by the NSA, which did not lead to action.

The USA Act, a financial law, and the Financial Anti-Terrorism Act were transmitted to the House of Representatives and the Senate on October 17, 2001, and placed in the Patriot Act as grounds for individual and collective surveillance mechanisms within and without American territory.

5.2. The United Kingdom

I) *RIPA*

A) *The Regulation of Investigatory Powers Act 2000*[11]: it regulates the jurisdiction of authorities that carry out surveillance and interceptions in the United Kingdom. It takes into account the development of the Internet and powerful encryption techniques.

RIPA can be invoked on grounds of national security, prevention of crime and public unrest, protection of public health and economic wellbeing.

It came into force on July 28, 2000. In September 2003, the Home Secretary at the time, David Blunkett, announced that the scope of application had been broadened. In 2000, only nine agencies could be referred to by RIPA, whereas in 2008, there were 792 agencies.

B) RIPA allows agencies the following:

– demand of an ISP, in secret, access to an individual's communications;

– monitor all electronic communications transiting through British territory;

– request that service providers upgrade their telecommunications devices in order to facilitate surveillance;

– demand that a person provide the code used to encrypt their personal information to the government.

11 2003 c 23

RIPA is applicable not only to electronic communications but also to connection data. The law garnered the approval of parliamentarians but was met with the opposition of human rights movements. RIPA was highly criticized by the majority of legal entities and private persons involved in human rights. Certain parliamentarians, concerned with the new role played by local councils, expressed reservations on the matter. Keith Vaz, Chair of the Home Affairs Committee in the House of Commons at the beginning of the century, claimed that RIPA could lead to abuses, seeing as certain files were "petty and vindictive". Brian Binley, another Member of Parliament, wished that local councils were not empowered by RIPA.

Moreover, articles 21 through 25 of RIPA created a system that authorized referenced organizations to access transmission data. Requests are made by a designated person and do not require the authorization of a judge. It was primarily designed for criminal investigations, national security and public protection. Guarantees are installed; a commissioner[12] monitors the exercise of powers conferred to the designated persons[13]. A court entertains the public's complaints. Collected intelligence is significant, whereas complaints submitted by the public are rare.

C) *Antiterrorism Crime and Security Act of 2001*

1) *The United Kingdom allows the collection and storage of connection data.* Information on the user such as their name, date of birth, telephone number, billing address, e-mail address, IP address, payment methods and credit card details can be retained for 12 months. Telephone information such as mobile and land line numbers, date of communications, time and length of telephone call and location of the respondent can equally be stored for 12 months. Information on Internet use such the date and time, the IP addresses and the URL addresses of websites visited can also be subject to storage measures.

2) *The United Kingdom's Anti-Terrorism, Crime and Security Act changed the length of storage of connection data of web users by service providers to at least a year*. This law anticipated the European directive of 2006, which in turn was invalidated by European jurisprudence in 2014.

12 Interception of Communications Commissioner.
13 Article 57, RIPA.

The Home Secretary claimed that he would have "the power to monitor online financial transactions and private e-mail traffic". However, controls dwindled rapidly, with the police being exempt from prior authorization from a judge on multiple occasions. The approval of the Home Secretary or one of their close collaborators was all that was necessary to act.

3) *Elizabeth France, the United Kingdom's Information Commissioner, stated*[14] *in 2002 that RIPA and the Anti-Terrorism, Crime and Security Act were sometimes at odds*. For example, the anti-terrorism law specifies that connection data may be retained "for a period longer than the needs of the operators but only if these data are necessary to investigations concerning national security". RIPA, on the other hand, allows access to data in many instances, the majority of which do not have the protection of national security as its aim, and without a legal warrant.

The Anti-Terrorism, Crime and Security Act of 2001, similarly to the American Patriot Act, allows for the indefinite detention, without charge or indictment, of foreigners suspected of terrorism. This detention has a distinctly administrative characteristic; if there is no evidence against the detainee, it is impossible to take them to court.

In December 2004, the Court of Appeals of the House of Lords condemned this unlimited administrative detention, as it is contrary to the European Convention for the Protection of Human Rights and Fundamental Freedoms. The judgment also found the difference in treatment of national and foreign citizens to be discriminatory. If the Court of Appeals of the House of Lords had not passed this judgment, a person taking legal action before the courts of the United Kingdom could, having exhausted all possible domestic remedies, file an individual application before the ECHR with a high likelihood of satisfaction.

4) *The Prevention of Terrorism Act*

The executive drew lessons from the Court of Appeals of the House of Lords. Discrimination is prohibited between national and foreign citizens. The Prevention of Terrorism Act, voted in March 2005, implemented a society of control. The Home Secretary could use electronic bracelets, house

14 August 2002 declaration.

arrests if a person was deemed "implicated in an act linked to terrorism", reduce the possibility of communications by forbidding the use of a mobile phone and give the police and secret services access to homes, and all of these at any moment. These provisions are made even in the absence of any kind of evidence, the advice of secret services being sufficient. The justification for the measures taken was the suspicion of a private individual and the scope of application of the law was practically limitless. The suppression of habeas corpus was extended to the totality of the population, without consideration of nationality. The Home Secretary possessed prerogatives previously devolved to magistrates.

The attacks in London on July 7, 2005 were highly mediatized, leading governmental authorities to exploit the events. They claimed that storing data for long periods of time was desirable: "Telecommunication records, whether of telephones or of e-mails, which record what calls were made from what number to another number at what time are of very important use for intelligence", declared Charles Clarke, the then Home Secretary in an interview with the BBC. According to him, it was essential to find the time a call was made or message was sent as well as those who made and received them. "We believe it is important to get a retention of data of what calls were made from some considerable time".

The United Kingdom asserted that rejection from the European Parliament, which considered the bill supported by the United Kingdom as well as France and Ireland, as "inappropriate and unreasonably severe" of the Framework Decision[15], had little judicial value. It was favorable to the retention of location data when communications were made through a mobile phone as well as the retention of the history of visited websites, IP addresses of people contacted through instant messages or a subscriber's correspondents' e-mail addresses, with the length of retention being between 12 and 36 months[16]. Thus, connection data storage was adopted.

5) *The Terrorism Act of 2006* was adopted in March 2006. This law created new offenses in terms of inciting terrorism. These incriminations did

15 Framework Decision on April 29, 2004.

16 The proposition was retained in the directive 2006/24/CE but with retention of 6–24 months.

not aim at the glorification or promotion of terrorism but rather, targeted individuals who, unwittingly perhaps, had participated in the creation of a climate favorable to terrorism. Opponents to the law remarked how this law gave British Courts the possibility to criminalize the support of political and social movements.

A new antiterrorist law adopted in 2007 empowered the police even further. Furthermore, the length of administrative detention was extended to 3 months[17] for people suspected of terrorism but with no incriminating proof or physical evidence against them.

In this backdrop of heightened surveillance, video surveillance, more than ever, played an eminent role in the United Kingdom. The Home Secretary made increased use of the thousands of cameras posted on streets and train stations, with citizens being tracked daily. They were not simply filmed but "analyzed". Video surveillance systems could be biometric or vocal. Experiments were carried out and exploited. As such, local authorities in Newham have possessed a video surveillance system since 1998 that was capable of facial recognition from a police database of known criminals and delinquents. Freedom of movement was constrained considering that an average Londoner was filmed at least 300 times a day, with the films likely to undergo meticulous exploitation.

On the basis of these texts and practices, mass surveillance is indeed a reality in the United Kingdom.

5.3. France

I) *The Law on Everyday Security (LSQ)*[18], was passed on November 15, 2001 on a proposition from the Jospin government. It contained a legislative package that grouped texts relating to various means to fight terrorism, trafficking[19], social nuisances and incivilities. The LSQ established the tools to fight terrorism using new technologies. It rendered the refusal to provide a

17 Previously 28 days.
18 "Loi sur la sécurité quotidienne".
19 Notably arms trafficking.

DNA sample an offense that incurred imprisonment, extending the field of application of the FNAEG[20].

A) *The LSQ allows municipal police, and no longer simply national police, to obtain a* "permanent authorization" from building owners and operators in order to enter into communal parts of buildings.

In terms of encryption, the Criminal Procedure Code, under the title "Clarification of encrypted data necessary for the establishment of truth", the judge may request a decryption of information by "the means of State under the secret of national defense", which is to say the army or the secret services.

B) *Furthermore, the LSQ imposes on people proposing a cryptography service* the obligation of providing their encryption algorithms to authorities.

The law allows for the storage of connection data for 12 months.

II) *The law on orientation and programming for internal security, called LOPPSI (loi d'orientation et de programmation pour la sécurité intérieure)*.

Published on August 29, 2002, it reinforces the policy focus on the fight against insecurity. It also allows officers of the criminal police, under the authorization of a magistrate, "to directly access computer files and to seize remotely, via telematics or computers, information that appears necessary to the determination of truth". It also provides for the fusion of STIC, the police database, and JUTEX, the *gendarmerie*'s database, under a single structure, ARIANE.

III) *The law on March 9, 2004, known as Perben 2*. This law has a generic aim of fighting delinquency and organized crime.

A) *It introduces the possibility of proceeding toward the interception of electronic communications during the preliminary investigation phase* for 15 crimes and misdemeanors. The request is made by the Public Prosecutor. The warrant is delivered by the judge of freedoms and custody (*juge des libertés et de la détention*) of the high courts. The warrant is issued for a

20 Article 56 of LSQ.

length of 15 days and is renewable once[21]. The severity of these crimes and misdemeanors is varied. What do "murder committed by an organized group", "acts of barbarism committed by an organized group" and "providing assistance to an irregular alien" have in common? It does not appear to be much. Nonetheless, it is possible to claim that these crimes and misdemeanors have an impact on public life, and have the potential to be mediatized.

B) *In terms of video surveillance, the investigating judge is empowered when necessary for the procurement of information, and on the advice of the Public Prosecutor, to authorize, by reasoned order*, police officers and agents to install video surveillance devices without the consent of the subjects for 15 crimes and misdemeanors. It is the police agents and officers and not the legal persons eminent in video surveillance that are responsible for installing the devices. The decisions must encompass all the elements allowing the identification of targeted vehicles and public and private places. The decisions are adopted for a maximal duration of 4 months. This duration corresponds to the length of telecommunication interceptions prescribed by the law on July 10, 1991. The residual difference remains in the renewability; legal telecommunication interceptions, at the investigative stage, are authorized for a length of 4 months, renewable without limitations. On the contrary, the system of video surveillance in the context of the March 9, 2004 law is installed within a deadline of 4 months. The investigating judge or the designated police officer must submit a report in which the recorded images are described that is useful in the determination of the truth.

The recorded images are only destroyed following prosecution.

IV) *Counterterrorism law on January 23, 2006*

When an urgent situation that exposes a risk of terrorism arises, the State representative at the department level and, in Paris, the *Préfet de Police* can authorize the installation of a video surveillance system without prior notice from the department-level commission.

21 This length can be carried to a month, renewable once, in the LOPPSI 2 on March 14, 2011.

The law also stipulates[22] that access to connection data by police authorities no longer requires the authorization of a magistrate, as had been the case previously, but leads instead to the work being carried out by police officers that are only held to account by a qualified entity chosen by the *Commission nationale de contrôle des interceptions de sécurité* (CNCIS). The independence of this entity is debatable as it is chosen by the CNCIS from a list of four people, established by the Minister of the Interior. The person chosen is highly connected to the Minister of the Interior, although meetings between them and the CNCIS are regularly held.

Because of the passage from a judicial control to an administrative control, a referral was made to the Constitutional Council at the request of parliamentary socialists. The Constitutional Council recalled[23] that the prevention of terrorism fell under administrative authority and repression under judicial authority, which was, in fact, a reminder of the principle of the separation of powers. The parliamentarians felt that this principle was being threatened, but this was not followed up by the Constitutional Council.

Initially valid until the end of 2008, this article was extended until 2012 by the only article of the December 1, 2008 law number 2008-1245.

The bill also provided that "anti-terrorist services of the police and the gendarmerie have access to certain administrative databases managed by the Ministry of the Interior" (databases concerning license plates, drivers' licenses, national identity cards, foreign passports, residence permits and visa applications database). The CNIL pronounced reservations and the bill was modified so that the access to the Ministry of Interiors databases can only arise under conditions fixed by the law on January 6, 1978, modified by the law on August 6, 2004.

Decree number 2007-86 on January 23, 2007, "relative to the access to certain automated processes mentioned in article 9 of the law no. 2006-64 of January 23, 2006, relating to the fight against terrorism and carrying various provisions relating to security and border controls", extended access to national databases of license plates, regulated by article L330-2 of the

22 Article 6.
23 Decision on January 19, 2006.

highway code by adding police, judicial and military agents that are directly concerned with road safety, "service agents of the Directorate-Generals of national police and national gendarmerie responsible for terrorism prevention assignments"[24]. This provision was supposed to end on December 31, 2008, but was extended until 2012 by a decree on December 30, 2008.

V) *Loppsi 2 on March 14, 2011*

The law on orientation and programming for the performance of internal security was succeeded by the Loppsi implemented between 2002 and 2007.

A) *Loppsi 2 reinforces the powers and authorities of the Minister of the Interior* for the anticipation, prevention, protection, combat and intervention against risks likely to jeopardize the institutions of the Fifth Republic, or threaten national unity, public order, people, goods, installations and resources of general interest. It tends toward the legal regulation of the modernization of security practices but also to "adapt our judicial arsenal to the evolution of threats that burden our internal security, spanning from organized crimes to minor delinquency, passing by cybercrimes or by the anarchical development of economic intelligence activities"[25].

B) *Loppsi 2 deals with adapting the law to new technologies*: databases are prioritized; the national DNA database[26], the automated fingerprint database[27] and missing persons database[28]. The possibility of using DNA is widened. It is suspended at the burial of an unidentified body in order to carry out the collection of scientific evidence, under the authority of the Public Prosecutor, in order to obtain identification before the burial or cremation of the body. Article 5 allows for DNA swabs to be taken from unidentified bodies or remains before burial or cremation.

The Public Prosecutor initiates the various measures necessary to obtain the deceased's identity.

Equally, the scope of application for recordings in the FNAEG is regulated. DNA collected during investigations on causes of death or

24 R330-2.
25 Jean-Christophe Lagarde, Assemblée nationale, third session, February 9, 2010.
26 FNAEG (*Fichier national automatisé des empreintes génétiques*).
27 FAED (*Fichier automatisé des empreintes digitales*).
28 FPR (*Fichier des personnes recherchées*).

disappearances, as well as DNA that is likely to correspond to deceased or missing persons can be recorded in the FNAEG. From 2003 to 2006, the number of recorded DNA profiles went from 2,807 to over 330,000.

Concerning the ascendants, descendants and collaterals of people whose identity is sought, such as parents or associates, their DNA can only be compared with the DNA of non-identified bodies and not with the rest of the database so as to not create confusion with results and equally in order to guarantee individual freedoms. Under these circumstances, the CNIL can act as a control.

A chapter that deals exclusively with judicial police databases was also created, allowing the recording of personal data of perpetrators, accomplices and victims of a crime, excluding the victims in legal procedures for the investigation on the causes of death or disappearances. The law proposed the expansion of the field of collected data to include background files of victims in particularly worrying investigations of causes of death or disappearances.

The objective was to expand the use of judicial police databases to the fight against delinquency in order to allow judicial police officers to benefit from the new comparison capabilities.

The national automated database on violent criminals and sex offenders[29] was created under the law on March 9, 2004 and aims to reduce repeat offense of sexual or violent crimes and facilitate the identification of perpetrators. Due to the recording of information, particularly the names and addresses of perpetrators, this database contributes to the rapid localization of sex offenders and allows district governments to control access to relevant professions. Upgrading was improved, and access was expanded, namely the inclusion of penitentiary establishments.

Finally, the law underwent an important modification to lower the threshold of crimes and offences for which serial analysis files were used.[30] Thus, aggravated theft, theft committed against particularly vulnerable

29 FIJAIS (*Fichier Judiciaire Automatisé des Auteurs d'Infractions Sexuelles ou Violentes).*
30 See ANACRIM, SALVAC.

persons and theft associated with acts of destruction or deterioration were also included.

C) *Another component of Loppsi 2 is dedicated to video surveillance, now the law on "video protection*"

It was deemed urgent by the legislator to finance a national plan to develop video protection and a specific plan for the video protection of Paris. The legislator wanted to triple the number of cameras in public places and develop video protection mechanisms that would satisfy the needs of police and gendarmerie services.

The bill considered authorizing the installation of cameras via private entities but this article was not accepted by the Constitutional Council, who claimed that this initiative needed to be undertaken by public entities.

The scope of application was extended, encompassing natural catastrophes and demonstrations likely to provoke public unrest, to be used in multiresidential buildings when serious harm could be done to people and goods, but only with the consent of the majority of coproprietors and in social housing, of building managers. Transmission occurs in real time and is limited to the time necessary for the intervention of police or gendarmerie services. It is based upon convention.

The commissions must maintain individual freedoms in this security process; as such it is necessary to evoke the role of the National Commission on Video Protection and that of the CNIL.

The National Commission on Video Protection was created by the decree on May 15, 2007[31] and was reformed by Loppsi 2.

The National Commission on Video Protection is composed of representatives of persons authorized to implement video protection systems, a CNIL representative, two deputies and two senators, and certain experts. There is an incompatibility between membership of the National Commission on Video Protection and possessing interests, direct or indirect, in a video protection company due to possible conflicts of interest.

31 Decree no. 2007-916.

The National Commission on Video Protection has as a general mandate the control of video protection. It writes recommendations of a technical nature on the functioning and use of systems of video protection to the Minister of Interior.

Administrative authorities, the Minister of the Interior, deputies and senators, video protection commissions at a department level may all come before the Commission for all questions relating to video protection. The Commission can exercise at any given moment, except in the sector of national defense, controls on the functioning conditions of authorized mechanisms and propose the suspension, if not the suppression, of mechanisms that do not conform to their authorization or whose use is considered abnormal.

With regard to the CNIL, it can, upon request of a department-level commission or from its own initiative, carry out a control aimed at ensuring that the video protection system is used in a manner conforming to its authorization as well as to the provisions under the law of January 6, 1978, which was modified by the law of August 6, 2004.

When the CNIL notices a failure in compliance to the provision, it has the right to issue a formal notice to order the system manager to end the malfunction in a period of time that they establish but which cannot exceed 3 months. If the manager cannot conform to this formal notice, the CNIL can issue a public warning. If these measures do not cause the cessation of the failure, the Commission can request from the State representative at the department level or in Paris, the Préfet de Police, an order to suspend or suppress the video protection system.

An establishment open to the public containing a system of video protection without authorization can be closed down for up to 3 months at the request of the department-level commission, of the CNIL, of the department-level State representative or in Paris, of the Préfet de Police, if the formal notice served to the concerned establishment has not had the desired effect.

The CNIL submits an annual public report to the National Commission on Video Protection, which details its activities in controlling video

protection systems and includes recommendations to remedy observed malfunctions.

Despite the new role to be performed by commissions, the important rise in video protection mechanisms as a product of the adoption of Loppsi 2 cannot be denied, even if France is not on the same level as the United Kingdom in terms of video surveillance.

Finally, LOPPSI 2 provides for remote computer data capture, justified by the need to dismantle networks and trafficking that sometimes rely on new technology. The grounds for this type of investigative process indicates that it was not intended to be used frequently but rather is reserved for "serious crimes" and terrorism. When necessary, the investigating judge can issue an order authorizing judicial police officers and agents with letters rogatory to install, without the consent of those concerned, devices whose purpose is not only to access computer data but also to record, store, transmit data in the way it appears on the computer screen for someone using an automated data processing system or in the way it is typed. These different operations are carried out under the authority of an investigating judge who can, at any given moment, order the interruption of the operation. The judge can authorize the installation of a technical device in a vehicle or private property, possibly outside working hours[32], with the permission of the proprietor, inhabitants or the vehicle owner. If the property is residential, authorization is given by the judge of freedoms and custody at the request of the investigating judge.

In order to install the device, the investigating judge can also authorize transmission through an electronic communications network, which requires the involvement of an electronic communications operator.

The investigating judge's decisions specify the offence that justifies the use of these measures, the exact location and a detailed description of automated data processing systems, failing which they would be invalid.

Decisions are taken for a maximum duration of 4 months. If necessary, data capture operations can, exceptionally, be extended for another 4 months. Only a single renewal is possible, contrary to what takes

32 6 am to 9 pm.

place with electronic communications interceptions at the investigatory stage.

The investigating judge or investigating officer designated by the former draws up a report on each of the implementing operations. This report includes the date and the time at which the operations started and at which they ended.

Computer data recordings are placed under closed seals. Data collected in a foreign language are translated into French with the assistance of an interpreter who is bound by an obligation of secrecy.

The recordings are destroyed at the request of the Public Prosecutor at the end of the public action; a dismissal therefore does not result in the destruction of recordings.

Loppsi 2, and particularly the "New information and communications technologies" component, contributes toward the rise of a secure society of which the limits were demonstrated by Mireille Delmas-Marty in [DEL 13]; "Is it enough to preserve freedoms in the face of the radicalization of social control? Made acceptable in the climate of fear created in the wake of the 9/11 attacks, these procedures must make unprecedented developments with… technologies that allow us to follow not only products but also people, into their private lives".

VI) *The antiterrorist law of November 2014*

In this section, several aspects related to digital technology, particularly in terms of a certain approach to the press, with a possibility of blocking Internet sites that promote the use of terrorism.

The freedom of press and the law of 1881 raise the question of the derogations concerning article 10 of the antiterrorism bill of 2014. The latter provides for a repression of "terrorist" propaganda.

The offences established by article 4, promotion or glorification and provocation, are exacerbated when the medium used is the Internet. Thus,

there is a debate concerning opportunity under this exacerbating circumstance. It is not the first time that an offence is associated with exacerbating circumstances when the medium used is the Internet, as it has occurred, for example, in the case of psychological harassment.

Another essential component is the administrative blocking of websites.

Administrative blocking already appeared in the context of LOPPSI 2 for child pornography sites, referring to the Convention on Cybercrime[33]. It resulted in a referral to the Constitutional Council that was not followed up. The provisions did not enter into force due to the absence of an implementing decree. Certain deputies and senators asserted that the fight against terrorism did not justify blocking websites, particularly administrative blocking. According to Lionel Tardy, "administrative blocking is a measure that can be dangerous for those who have nothing to do with terrorism, and is entirely counterproductive in the fight against those involved in that are"[34].

The implementation decree on February 5, 2015[35], as was envisaged, relates to the administrative blocking of terrorist and child pornography websites. A joint effort was set up between the central office against crime using information and communications technology. Even with this decree, however, the problem of technical security is far from being resolved. Internet providers are communicated a list of websites to block by intelligence services if the latter are unable to shut down the sites through the website's editors or hosts.

The director of the National Agency of the Security of Information Systems[36] expressed his/her reservations during a conference organized on September 10, 2014. These reservations were primarily technical. As a result, a delay in the implementation of a block has to be taken into consideration. Furthermore, is it necessary to undertake blocking on behalf

33 November 23, 2001, France signed and ratified this text.
34 Lionel Tardy, Assemblée nationale, second session of September 17, 2004.
35 Decree no. 2015-125 on February 5, 2015 relative to blocking Web sites that provoke or promote acts of terrorism or Web sites that diffuse pornographic images and/or representations of minors.
36 *Agence nationale de la sécurité des systèmes d'information* (ANSSI).

of the host and the domain or through the intermediary of URL filtering? The implementation decree refers to both domain names and host names. The solutions adopted, however, must not block legal content that is not targeted by the law. This does appear to be possible. The majority of actors represented by the National Digital Council and the Commission on the reflection of rights and freedoms in the digital age (*La commission de réflexion sur le droit et les libertés à l'âge du numérique*) share these worries. The devices used for blocks using IP addresses, domain name or even URL are not neutral. Anonymization techniques are relatively easy to use and can be overridden. Blocking devices are likely to induce "overblocking" on websites that are not targeted by the blocking measures, which can create a danger for the resilience of a network.

Furthermore, the law stipulates that hosts and ISPs must install devices that signal illegal content relating to terrorism. The Constitutional Council has already made note of the "frequent difficulty in establishing the legality of the contents". This is particularly salient when considering the "glorification" of terrorism. In 2004, the law relating to confidence in the digital economy abandoned the surveillance obligations for hosts and since jurisprudence has not ceased to fluctuate on the criminal responsibility of hosts.

In terms of interceptions, article 20 of the law on December 18, 2013 concerning military programming introduces data on geographical localization into security interceptions. The requests are initiated by the Interior, Defense, Customs Ministers as well as the Budget, Economy and Finance Ministers. Authorizations are made by the Prime Minister[37].

Article 15 of the antiterrorism bill stipulates that the maximum delay in which recordings must be destroyed is 30 days. Indeed, the amount of data has increased exponentially and transcriptions are more complex, namely due to passing monitoring from lines to targets. Certain analyses require more time seeing as some interceptions involve languages not often used or complicated decryption. At the Senate, it is the CNCIS that decides whether a delay may be extended to 30 days, a decision entrusted by the Law Commission. The joint committee decided upon the suppression of article 15. This question, among many others, was covered in the law relative to the

37 Previously made by 10.

reform of the intelligence sector, which, for several months, gave rise to comprehensive studies.

Due to this law, the accelerated procedure was questioned, giving rise to parliamentary debates on limits.

Moreover, blocking alleged terrorist websites through an administrative route has been strongly criticized, namely by the National Consultative Commission for Human Rights, which was favorable to the presence of a judicial judge during the process and a subsidiarity that would allow for the implementation of incremental measures against potentially illegal content. The requirements for freedom of expression can be demonstrated in the following: "While freedom of expression can be restricted on grounds of national security… any such restriction must not only be necessary to achieve that aim but must also be proportionate"[38].

Security laws take into consideration several technical arrangements: digitization and interceptions, biometrics, scanners, drones, etc.

38 Human Rights Watch, October 9, 2014.

6

Interceptions

Interceptions are decided at a State level, but often international interceptions are also allowed.

6.1. The United States of America

This is, in particular, the case in the United States which, via lawful interception, captures data throughout the entire world.

I) *Terrorist surveillance program*

This was set up by the Bush Administration after the September 11, 2001 attacks and the adoption of the Patriot Act. Its lawfulness has been questioned to the extent that it has not received the approval of FISC[1].

II) *PRISM*

A) *An American electronic surveillance program named US-984XN*[2] *collects information from the Internet and from electronic service providers*. This is a classified program and it falls under the supervision of the National Security Agency; it is used to target people who live outside the United States, which is made in conjunction with the Upstream Program. Prism was

1 United States Foreign Intelligence Surveillance Court.
2 ZDNet, "Prism: Here's How the NSA Wiretapped the Internet", June 8, 2013.

Security and Privacy in the Digital Era, First Edition. Claudine Guerrier.

authorized[3], unlike the Terrorist Service Program, by a ruling of the FISC[4]. So there is a presumption of legality from the American law perspective. In accordance with this system, the National Security Agency (NSA) has direct access with data that is notably hosted on Google, Facebook, YouTube, Microsoft, Yahoo, Skype, AOL, Apple and Paltalk[5]. Prism would be "the first source of raw information used to draw up the analytical reports of the NSA"[6]. Certain companies are reluctant to provide calls from their clients; in general, in these companies, when classified information was disclosed and gave place to controversies, they claimed that it was off the table for them to transmit bulk information to the NSA, and that, under U.S. law, they were obedient to the rule: the information request should involve those individuals and it should be in compliance with FISA law.

B) If, at a geopolitical level, it may seem expensive to intercept the information of allied representatives, this does not make it less part of the balance of power established within the Western bloc and the statements widely publicized by Viviane Reading or Martin Schultz, which reveal an internal use of communication policy.

On the contrary, *the compliance of PRISM under FISA law and the evolution of the FISA law constitute an essential issue for American law* and, to a lesser extent, international law.

It is important to mention the legislative decree from 2002, the jurisprudence, and the FISA law reform.

III) *The legislative decree from 2002*

A) *Since 2002, it has no longer been necessary in the U.S., in certain instances, to seek and obtain judiciary authorization to run interceptions*. In 2002, President Bush signed an executive decree authorizing the National Security Agency to monitor and intercept outbound telephone calls and

3 The Washington Post, "NSA Slides Explain the PRISM Data-Collection Program", June 6, 2013.
4 Its creation was permitted by Protect America Act of 2007, under the presidency of George W. Bush.
5 Glenn Greenwald and Ewen MacAskill, "NSA taps in to systems of Google, Facebook, Apple and Others, secret files reveal", The Guardian, June 7, 2013.
6 The Washington Post, June 6, 2013 (see: below).

international e-mails sent by people in the United States to people outside the U.S. and vice versa, without having to request prior judiciary authorization from the FISA court[7]. The President would have received the power required to take this decree according to the ruling granted by article 2 of the American constitution[8] and in accordance to a joint resolution by both Chambers of Congress, issued by the Senate[9], holding the title of Authorization for Use of Military Force (AUMF). The AUMF resolution authorized the President to use all the necessary and appropriate force against the States, organizations or people, who, according to him, had planned, committed or favored the September 11 attacks or sheltered those who committed this actions in order to prevent potential or future terrorist actions.

B) *Nonetheless, certain groups and certain individuals wondered if the president actually had the constitution power or authority granted by Congress to assume the decree from 2002*. They especially asked the following premise: is the electronic surveillance exerted by the NSA, without any warrant, a violation of the rights of Americans according to the Fourth Amendment? Studies have been conducted on this topic[10].

Furthermore, certain observers have questioned the government's claim that the decree from 2002 was necessary under the pretense that longer warrantless periods of surveillance than those authorized by the FISA are needed in order to prevent and fight said terrorist activities. Indeed, although governmental agencies in general must obtain a FISA court authorization before performing warrantless surveillance, the FISA provides exceptions to this requirement. The U.S. Attorney General can order electronic surveillance of certain foreign powers without any judiciary order during a maximum period of a year[11]. Warrantless electronic surveillance in

7 E. Lichtblau and J. Risen, "Bush Lets US Spy on Callers Without Courts", The New York Times, December 18, 2005.
8 This article specifies the Executive Powers of the President, and encompasses the corresponding powers as a chief of the American Military Forces.
9 SJ Res 23.
10 See the brief by Elizabeth Bazan and Jennifer Elsea, "Presidential Authority to Conduct Warrantless Electronic Surveillance to Gathers Foreign Intelligence Information" also see, M.H. Halpern, "A legal Analysis of the NSA Warrantless Surveillance Program", January 5, 2006.
11 50 USC 1802.

emergency situations for up to 72 h is also possible[12] as well as warrantless electronic surveillance for 15 days after a declaration of war by Congress[13].

IV) *Jurisprudence*

On January 17, 2006, two separate prosecutions were launched against the warrantless surveillance program, the first started by a group of organisms protecting individual liberties led by the ACLU[14] before the Detroit Federal District Court against the NSA, the second one conducted by the Center of Constitutional Rights against President Bush, the NSA and the FBI in Manhattan's Federal Court. According to the group led by the ACLU, the NSA program violates the First and Fourth Amendment of the Constitution, the constitutional principles of separation of powers. The group demands that the program be declared unconstitutional and that an ordinance should prohibit the NSA from continuing its activities in this area. The proceeding requested by the CCR states that data protected by the attorney/client relationship were intercepted within the framework of the NSA's warrantless surveillance program and recaptures the claims from the ACLU with regard to the constitutional violations. Just as the ACLU, the CCR demands a declaration of unconstitutionality and an ordinance prohibiting the continuation of the program.

The debate gained the parliamentary spheres. When the information concerning the warrantless monitoring program of the NSA and the authorizing decree was made public, various committees from the Congress have advocated toward a survey about the program and the power that would be given to the President under the Constitution or the AUMF resolution to authorize the NSA to conduct warrantless surveillance, while FISA has not amended any law. On January 15, 2006, the President of the Senate Committee of the Judiciary, Arlen Specter, announced that his committee would hold hearings on these issues. Nonetheless, Arlen Specter provided no pointers about the number of hearings, the quality of the witnesses. Since the statements of Senator Specter, the SCJ has effectively conducted its survey

12 During this 72-h period, a warrant authorizing such surveillance is requested to the FISA Court, see: 50 USC 1805(f).
13 50 USC 1811.
14 American Civil Liberty Union.

and is particularly interested in the legality of the program. On February 6, 2006, the SCI heard Attorney General Gonzales: the latter supported the position of the executive; the President is empowered to authorize the NSA's warrantless surveillance program and he holds this power under his attributions as Commander in Chief, according to article 2 of the American Constitution and the AUMF resolution. The SCI then held two additional hearings concerning the executive power during wartime and the NSA's surveillance power, on February 28 and on March 28, 2006.

Justice was ruled on two occasions. In August 2006, the Federal Judge Anna Diggs Taylor, based in Chicago, had validated a complaint filed by lawyers, teachers and journalists, who were in constant contact with the Middle East and who believed that their communications were subject to monitoring. Considering that President Bush had exceeded his powers by allowing the alleged surveillance, Judge Taylor demanded the immediate termination of the program. This was appealed and the decision of Judge Diggs Taylor was suspended waiting for the Court of Appeal to rule. In July 2007, the order to stop the "antiterrorist" interceptions in the U.S. without any warrant by a judge was annulled by a Federal Court of Appeal. This decision allows, once again, the President to be free to continue the interceptions without a warrant from a judge.

V) *FISA's Reform*

A) *The law on August 5, 2007*

The law promulgated on August 5, 2007 reforms FISA. The American government could already spy on foreign communications that did not transit through the United States. Now, the NSA can, without a warrant, intercept telephone calls and e-mails of foreign nationals transmitted using American equipment. Some opponents have pointed out the dangers of excesses; they noted that it was now possible to intercept Americans communicating with people overseas without wrongful or criminal intent. However, a guarantee exists.

If an American becomes the main target of interceptions, a warrant is required to continue monitoring. The FISA court, in this context, no longer plays a significant role and the control by an independent agency of the U.S. government is experimented. Emphasis is placed on the fact that this reform from 2007 was only valid for 6 months. It is therefore necessary to consider

the debates that followed the end of the first decade and the beginning of the second decade of the 21st Century.

B) *The law of 2008*

In light of the discussions that arose concerning the previous program and the law from August 5, 2007 that allowed warrantless interceptions, a law was introduced and adopted by the Representatives Chamber and the Senate on July 10, 2008[15]. This law authorizes American intelligence to practice, without prior authorization, interceptions of electronic communications abroad in the grounds of spying or terrorism. The text allows a 1-year term to be obtained for interceptions of groups and foreign individuals. Meanwhile, an American citizen can be intercepted if there are foreign communications involved. Nowadays, authorities have a week, and not 72 h, to obtain a warrant. They must obtain the approval of the special court established by law to intercept the conversations of an American abroad, whereas before the approval of the Minister of Justice was enough. Hence, the protection of personal privacy is reduced, and for this reason a supervisory body is set up. "The Senate passed a good legislation authorizing Intelligence to listen in a timely manner the conversations of foreign terrorists in order to defend the freedom of the U.S." can be read in a statement broadcasted by the press service of the White House.

The law grants legal immunity to American operators of electronic communications accused by American justice of working with the government and secret services to engage in unlawful interceptions. In 2008, in spite of the judgment of the Federal Court of Appeal mentioned above, a quarantine of requests recollecting several billions of dollars was engaged in the context of telephone interceptions in the United States. The initial project did not mention judiciary immunity but it seemed essential to the executive and the electronic communication companies. President Bush informed that he would not wait for the discussions to come to an end in order to authorize the surveillance of communications[16] of suspected terrorists. To justify this attitude, the President invoked possible threats against national security. As a result, electronic communication operators should not have to pay damages to those who accuse companies of violating their private lives: "To be able to

15 By 69 votes, including that of Obama, against 28.
16 Telephone conversations and e-mail exchange.

discover… the enemy's plans, we require the cooperation of telecommunication companies… If these companies are subject to lawsuits that may cost them millions of dollars, they will not participate. They will not help us. They will not help protect America". Once the legislation is passed, the hypothetical control by the judiciary is out of reach for all citizens.

The extension of the FISA law until 2015

On September 12, 2012, the U.S. House of Representatives voted[17] for a 5-year extension on the FISA law. This law should have expired on December 31, 2012. "Once again, the House endorsed a law so broad and vague that, despite its vote four years ago, we have no idea how the government uses it", declared Michelle Richardson[18]. Mrs. Richardson adds that Americans and their communications are protected from intrusion of the executive, in theory, by the Fourth Amendment of the Constitution. Senator Ron Wyden said that Congress was entitled to obtain information about the number of Americans who have had their conversations intercepted under the authority of the FISA law. Ron Wyden has also denounced the shortcomings of the FISA law concerning individual liberties. Furthermore, always in 2012, the Electronic Frontier Foundation expedited prosecutions in the Federal District of Columbia considering that the NSA has not met its obligation of protecting American citizens. Despite the actions conducted by the ACLU, the Electronic Frontier Foundation, some Senators and House Members and Representatives, the law is definitively passed by the Senate in December of 2012. Ron Wyden insisted in vain on the prerogatives of the American government under that law, which allows targeting any political entity or organization considered as a policy-foreign organization. This affects foreign legal and natural persons, enemies of the United States and also foreigners belonging to countries that are allies of the United States, Canada, countries of the European Union, Australia, etc. Because of the FISA law, the American government is able to request data from large U.S. companies by issuing a classified mandate that requires companies to cooperate with intelligence services. Within the European Union, the Center on Conflict Studies, Freedom and Security[19] published a report[20] in January,

17 301 favorable votes, 118 unfavorable votes, 10 abstentions.
18 Legislative Counsel of the American Union of Civil Liberties.
19 Fighting cyber crime and protecting privacy in the Cloud.
20 Report commissioned by the Committee on Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament.

2013, which denounces the FISA law and stresses the nuisances and drifts in this law. The Patriot Act and the FISA law are questioned: “The issues of respect of personal privacy and data protection are raised by the exceptional measures taken in the name of security and the fight against terrorism. We must emphasize here the peculiarities of American context, as a result of both the Patriot Act and the new FISA law. These aspects were completely overlooked despite their considerable implications in terms of European sovereignty over the data and the protection of the rights of its citizens”.

VI) *It is important to take into account that the outsourcing generated by the Cloud is used more and more frequently*. When the possibilities of the Cloud are combined with the provisions of the Patriot Act and the FISA law, the liberties of foreigners are potentially threatened. Experts from the Center on Conflict Studies, Freedom and Security warn politics and legal practitioners of the European Union: “Particular attention should be paid to American laws authorizing the monitoring of data stored in the Clouds by non-US residents. The European Parliament should demand preciseness about the FISA law, on the new situation posed comprising the Fourth Amendment of the American Constitution, and the Patriot Act (particularly Article 215). The European Parliament should consider modifying the regulations in the domain of data protection, so that appropriate warnings are addressed in terms of personal information (or information vulnerable to political surveillance) prior to export data in the Cloud, toward American jurisdictions... The European Parliament should reopen negotiations with the U.S. so that the right to personal privacy is recognized by American courts in its European sense”. In fact, the current power relations between the United States and the European Union are not favorable toward renegotiation. The United Kingdom adopts almost all diplomatic positions of the United States, participates as an ally in its war efforts; France has not only reinstated the military bodies of NATO, left behind in 1966, it has also played a forefront role of Western allies in Africa, particularly in Libya and Mali. This reinforced involvement of the United Kingdom and France, both nuclear powers in the Western military alliance, suggests close cooperation between intelligence services and, *de facto*, the pre-eminence of the NSA and the FBI, included the framework of interceptions. It is illusory to think that the nation states want to question the legal foundations set up by successful

American executives. According to Sophia Helena in't Velt[21]: "It is clear that the European Commission prefers to look elsewhere. Just like national governments; notably because they do not understand the issues, and also because they are afraid to defy American authority…".

A) The Fourth Amendment of the American Constitution, by definition, concerns only American residents and foreigners are not capable of invoking it in order to obtain protection.

The procedural requirements that must, according to the FISA law, be respected by the police or intelligence services in order to obtain information that are not substantial. The personal privacy of foreign citizens and their personal information, even if they are not "terrorists" or "enemies" of the American government, are potentially monitored and the generalization of the Cloud solution does not improve the situation.

In this context, PRISM seems very consistent with the FISA law and the provisions of the Patriot Act. The compliance of PRISM toward the Fourth Amendment to the American constitution remains in question.

B) Furthermore, the data presented as foreign in the United States, often European, is not necessarily foreign: even if the data involve European residents and is therefore subject to the law of the European Union, *hosting these data in the Cloud by an American corporation or by servers established in the United States adds an attachment to American law*. The United States logically applies its national law to the activity taking place on their territory and the companies headquartered in the country. This is why a European state cannot blame the United States for wanting Google to transmit data according to the U.S. law and at the same time demanding that Google respects the rights of European countries[22] on the grounds of data processing for the services that it proposes. When it comes to data processed by a public entity[23], the relationship between the data subject and the entity mentioned above results as a basic principle of the law and it is very rare that this law allows the entity to expose data on the conditions of a

21 Vice President of the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament in 2013.
22 More protective than American law with regard to privacy and personal data.
23 See: public school, administration.

foreign law. However, this is what happens when foreign service providers are used.

It is convenient, nonetheless, to establish a distinction between data that are not personal data. When data have a personal nature, the cloud-based solution should be examined with attention and caution. Then, there is a risk for foreign data posed by American law, especially as the majority of European intelligence services cooperate with American intelligence and accept the interference provided against foreigners by American law. Currently, there is an interaction between lawful interceptions, albeit classified, under American law and the planned European regulation, which is substituted by guideline 95/46/CE.

The media discussion of PRISM has resulted in some changes in positions on this text. The latter contains specific provisions for the transfer of personal data outside the European Union. These provisions could turn out to be deterrent against American companies that could transfer European data to the United States. The proposed sanctions in case of violations of these provisions could "go up to 2% of the worldwide turnover of companies like Google or Facebook in case of violation", which would be far more deterrent than the planned $100,000 or $200,0000 in case of violation of American law.

C) *Finally, this process can participate in the renegotiation of the Safe Harbor Principles*. On August 13, 2013, the G29 contacted by mail[24] the Vice-President of the European Commission to consider and analyze the consequences of the PRISM program over the data protection of European Union citizens. A working group between the United States and the European Union was established with reference to the access by American intelligence services to the data of European Union citizens; this group notably includes members of some data protection authorities, legal and technical experts, of European and American descent in the field of counterterrorism; however, the G29 believes that it deserves to independently assess the possible violations to the sources of law of the

24 Mail sent on August 13, 2013, by the President of the G29, Jacob Kohnstamm, to Commissioner Viviane Reading, with a copy to Ccilia Malmström, another European Commissioner, Martin Schulz, then President of the European Parliament, and Juan Fernando Lopez Aguilar, then President of the Commission of the European Parliament.

European Union. The main objective of G29 is to engage in an analysis of comparative law to determine to what extent American legislation is or is not in accordance with international law and the law of the European Union: this is in order to address the kind of information that has been collected, on which conditions has the United States accessed such data, on the controls that exist in the United States, the review procedures for residents of the European Union. The G29 also intends to list the European surveillance systems similar to PRISM: "It is important to ensure that the European states are mindful of the fundamental right to privacy" reads the G29 in a statement released in August of 2013.

In France, the CNIL appealed to the French government so that data were transmitted over a data collection program. It also established a working group in relation to the access by foreign authorities to data belonging to French citizens.

D) *In the United States, an internal audit*[25] *was conducted by the NSA*. The audit revealed that the NSA has committed numerous breaches of law against the respect of personal privacy since it was given its new powers. The NSA reportedly ordered its members to falsify reports addressed to the Justice Department and the office of the Director of National Intelligence and would have substituted certain minor details by much more general ones. The NSA would have also hidden the unintentional surveillance of some American citizens. For example, a significant number of calls from Washington were monitored as a result of a programming error that switched the prefix of the American capital region[26] with that of Egypt[27]. Data were also collected and stored by an optical cable in American soil, and communication data from American citizens were collected in this opportunity, which is prohibited.

According to the NSA: *"*When we make a mistake (…), we point it out internally and to federal operators and go to the bottom of the problem.. Activities would be "continually audited and supervised internally and externally"[28], dysfunctions, according to John DeLong[29] are "errors and not

25 From May, 2012.
26 202.
27 20.
28 NSA quoted by the AFP on August 16, 2013.
29 Director in 2013 of the Internal Control Department of the NSA.

deliberated infractions" and the error rate would be of 0.0005%. Furthermore, when interviewed by Reuters on August 20, 2013, the NSA indicated that its mission "is concentrated on the fight against foreign enemies who want to harm the country" and "we defend the United States against such threats while relentlessly working to protect the personal life of Americans. It is not one or the other. It is both at the same time". In contrast, Senators Ron Wyden and Mark Udall[30] declare in a statement: "We have said that the violation of laws and rules were more serious than recognized and we think that Americans should know that this confirmation is only the submerged part of the iceberg".

E) *The NSA is controlled by the Congress and the FISC*, whose mission is to oversee the NSA's surveillance programs. The reports received by Congress are not complete: if Parliament representatives want to be aware of non-redacted reports, and if they have a defense clearance, they are obliged to use secure rooms to view these documents, but even parliamentarians who have this defense clearance are not allowed to take notes. As for the FISC, it does not always receive comprehensive information. Its President[31] stated "The FISC is forced to rely on the accuracy of the data that is provided to it" and emphasized the absence of power of investigation allocated in this body. The Senate organized a hearing in 2013 regarding the interceptions, in particular those of American citizens. "I continue to worry about the fact that we do not receive any straight answer by the NSA" explained the President of the judiciary commission of the Senate[32].

However, PRISM is not questioned by the American Executive. According to James Clapper, main representative of American intelligence agencies, PRISM is not the source of interceptions of e-mails or interceptions of American phone conversations.

On August 10, 2013, President Obama announced a reform of laws and policies that encompass the surveillance of citizens over the Internet. He wanted more transparency. This implied modifying, while working in coordination with the Congress, certain dispositions of the Patriot Act, particularly section 215, relating to the collection of metadata. The

30 Of the Intelligence Commission.
31 At the time, Reggie Walton.
32 Patrick Leahy.

knowledge of metadata allows the privacy of a citizen to be violated, similar to the illegal use of personal data.

In the American market and the international market, the capture, legal or illegal, of metadata induced privileged access to multiple information relating to individuals and can be subject to civil or commercial exploitation. While requesting his wishes for more transparency, Mr. Obama denied that the Patriot Act and the FISA have led to abuses. He foresaw the disclosure of more information on a dedicated website and the appointment of a representative of civil liberties to ensure independence in the intelligence surveillance court abroad[33].

On August 10, 2013, Mr. Obama was also committed to establishing a group of experts in order to audit and evaluate communication surveillance programs conducted by the United States. This audit is external to intelligence agencies, although different from the internal audit conducted by the NSA on May 2012 and that had, nonetheless, permission to enumerate 2,776 incidents over the previous 12 months concerning the collection, storage facilities, accesses and legally protected data communications.

On August 12, 2013, James Clapper become in charge of forming the group of experts that are taking care of the audit. Taking into account his previous functions, could it really be independent? The question was asked. Provisional conclusions were made within 60 days; final conclusions are to be provided before December 15, 2013.

Many elements seem to indicate that this was primarily a communication operation.

Mr. Clapper is placed directly under the statutory authority, due to his position, of the President of the United States. Moreover, in the recent past, James Clapper lied to Congress, which is serious under American law. He indicated to Congress that the NSA program had provided “no data in regards of Americans”. Since then, James Clapper has acknowledged that this response was “clearly erroneous”.

Furthermore, experts must assess whether intelligence activities “optimally protect national security and support our foreign policy”, they also need to measure “the risk of unauthorized disclosure or the need to

33 Foreign Intelligence Surveillance Court.

maintain public confidence". The language employed is rather vague, which creates legal uncertainty.

Finally, there is no mention among the experts of any foreign person regarding intelligence services.

PRISM seems relatively consistent with American law, but it is not reported on the status returned to intelligence agencies working on behalf of the nation state to which they are bonded, and sometimes in collaboration with intelligence agencies of other nation states.

6.2. France

It went through a significant legal evolution related to interceptions between 2013 and 2015. It is important to mention beforehand the possibility of recourse within legal framework, in the recordings of images and sounds and capturing of remote computer data.

I) *The capture of images and sounds was introduced by the criminal procedure code by the law dated December 12, 2005*[34].

A) *When the necessities of information demand it and are within the scope of article 706-73*, the examining magistrate can, after consulting with the prosecutor of the Republic by reasoned order, authorize officers and agents of the judiciary police employed by the rogatory commission to set up a technical device with the purpose, without the consent of the interested parties, of capturing, fixating, transmitting and the recording of spoken words by one or many individuals privately or confidentially, in public or private places or vehicles, or the image of a person or many people in a private space. The crimes and offenses are those specified in the Perben two law from March 9, 2004.

B) *Certain exceptions are anticipated as follows:*

– the recording of images and sounds can be made outside of the periods mentioned on article 59 of the Criminal Procedure Code[35];

34 Law no. 2005-1549 from December 12, 2005.
35 Article 59 of the criminal procedure code states that searches may take place before 6 in the morning or after 24 h.

– the installation or recording can be done without the knowledge or consent of the owner or possessor of the vehicle or the occupant of the locations[36].

The implementation of the technical device excludes certain "protected" individuals due to their duties. These are as follows:

– *Lawyers*: the implementation of technical devices cannot take place in pursuance to the premises referred to in Article 56-1 of the criminal procedure code.

– *Press organizations or broadcasting companies*: the implementation of technical devices that capture sound or images cannot take place in the premises referred to in Article 56-2 of the criminal procedure code.

– *Doctors, notaries, solicitors, bailiffs*: the implementation of technical devices that capture sounds or images cannot take place in the premises referred to in article 56-3 of the criminal procedure code.

– *Members of the Parliament or Senators*: the implementation of technical devices to capture sounds and images cannot take place in the homes of the persons referred to in Article 100-7 of the criminal procedure code.

If the technical device is installed in a living space and the operation occurs before 6 or 24 h, the liberty and custody judge should issue the authorization of installation.

II) *The capture of remote computer data* is laid out by LOPPSI 2 dated March 14, 2011 and introduced in Articles 706-102-3, 706-102-7, 706-102-9 of the criminal procedure code.

The system allows an investigator to access without the consent of the interested party to computer data "as it appears on a screen for the user of an automatized data processing system or as he/she introduces it through character entry"[37]. It is possible for the police, in accordance with procedures, to install cookies on computers of individuals suspected of

36 Article 706-96 of the criminal procedure code.
37 Article 706-102-1 of the new criminal procedure code.

having committed crimes or felonies, whether gang related or in an organized manner, under the law of March 9, 2004, or, if it is impossible to have physical access to the computer, set up cookies, a software that is able to retrieve the contents of some files and transmitting this content to a predefined destination over the Internet or "keyloggers" software whose purpose might be to capture the keys pressed by the user or record them into a folder and send over this folder to a predefined destination over the Internet[38].

Previously, it was necessary, in order to access computer data, to request permission from Internet access providers, and investigators were not able to capture encrypted conversations. Moreover, some devices do not leave traces of data in mainframes.

The vast majority of commercial companies are not involved in capturing computer data: LOPPSI 2 authorizes the use, ruled by the examining magistrate, of this process, when there is a computer exchange among members of a delinquent or criminal organization, which rarely occurs. This technical device does not apply to any of the persons mentioned in the law from December 12, 2005 with regard to the capturing of images and sounds.

III) *On December 18, 2013, the law of military program was enacted*, dedicated to the future of the French army, and also geared toward an amendment of the plan of interceptions of electronic communications. The latter is addressed in section 20 of the law.

The initial article (13th) focused on geolocation. It was expanded to the interception of electronic data. The Senate's initiative was taken in Commission by the National Assembly on the occasion of the review of the law for military planning. Geolocation is susceptible to follow the movements of mobile phones and people who own them, at regular intervals or in real time. Yet, the old writing of article L34-1-1 implied that the requests could only be made to the retained data, meaning that after using a mobile phone, made impossible real-time monitoring of a "target" service. It was convenient to address the shortcomings of this situation. Real-time

38 The explanatory statement of Article 23 explains that "computer data capture is considered essential to dismantle trafficking networks that use sophisticated techniques".

geolocation is now attached to administrative interceptions. It is the Prime Minister who issues the authorization and the CNCIS who delivers its opinion. The maximum duration of surveillance is, for the first time, 4 months, for the second time, ten days and discussions take place during this time; certain parliamentarians or officials of intelligence services claim this duration is too short, other parliamentarians beg to differ[39]. An amendment extends the maximum duration to 1 month.

A) *First of all dedicated to geolocation*, article 13 and then article 20 of the law of military planning is extended to data connection interceptions.

B) *Law no. 2006-64 from January 23, 2006* introduced, within the regulations of postal and electronic communications, article L34-1-1, which allows authorized individuals to require electronic communication operators the transmission of data connection.

Article 32 of the Law from January 23, 2006 anticipated that these provisions were applicable until December 31, 2008. Law No. 2008-1245 from December 1, 2008 that extends the application of articles 3, 6, 9 from the law of January 23, 2006, prolongs this application 4 years, which means it is extended until December 31, 2012, afterwards, law no. 2012-1431 from December 21, 2012, relating to security and the fight against terrorism extends these dispositions until December 31, 2015. These texts imply the compulsory referral of a qualified person placed under the assistance of the Minister of the Interior, the installation of the platform of the coordination unit of antiterrorist fight[40] and a subsequent control of the CNCIS.

The ordinary law measure in regard to the security interceptions is not that of article L34-1 from the code of postal and electronic communications,

39 "...In regard to geolocation, I would first like to recall that in the field of fighting terrorism, we need to proceed to conduct surveillance in hostile environments. Yet it is very difficult to deploy personnel on the ground for several hours in the same place without being detected. It is therefore necessary to use technical means to know where the person who is the subject of our investigations is in real time. This is what allows geolocation.... Given the methods currently being used by persons subject to investigation, we must give intelligence agencies the means to act: I do not understand why would we limit the right to proceed to geolocations to a ten-day period, however we allow clearly more intrusive telephone interceptions during four months" Patrick Calvar, Central Director of Internal Intelligence, National Assembly, November 6, 2013.
40 UCLAT.

which takes into account connection data, but that of articles L241-1 and the following ones from the code of internal security.

The text from the Senate regroups, in a new Chapter 6, Title IV of Book II of the Code of Homeland Security articles relating to the administrative access to connection data, which is found in the same article as those relating to security interceptions.

The system covers include connection data and geolocation in real time at the same time. It extends the capabilities of accessing these data to all intelligence services, which is made for reasons related to the defense of the basic interests of the nation.

C) *The requests of agents are always reasoned* and subject to the decision of a qualified person under the supervision of the Prime Minister, appointed by the CNCIS, on the proposal of the Prime Minister, who presents a list of at least three names. If the CNCIS considers that the acquisition of a connection data was authorized in infringement of legal grounds, this issue makes for a recommendation of the prime minister requesting an end to the connection data acquisition[41].

The new article L 246-2 of the internal security code establishes all information and documents to be requested by the designated officers and duly empowered services associated with the ministers in charge of internal security, defense, economy and budget. The ministry of economy and the ministry of budget were not previously in charge of security interceptions; however, they could already access technical connection data after a case of the CNCIS from 2010: the CNCIS considers that the detailed invoices and identifications fall under the preparatory phase of the interception. Article L 246-2 from the internal security code revokes articles L 222-2 and 222-3 of the code of internal security that made it possible for policemen and cops to access data held by electronic communication operators[42] or data retained by communication service providers to the online public[43].

41 This recommendation is also brought up to the attention of the Minister, who is responsible for the request.
42 Article L 222-2 from the internal security code.
43 Article L 222-3 from the internal security code.

The new article L 246-5 states that the identified and specific additional costs incurred by the operators in order to be able to satisfy the data connection requests lead to financial compensation.

The Parliamentary Assembly refers to two important rulings of the court of cessation from October 22, 2013: "The Court of Cassation has decided that the use of geolocation as part of a preliminary investigation was unfounded when it was requested by a prosecutor on the grounds that it cannot be learned by an independent judge, at any rate, not according to the jurisprudence of the CEDH"[44]. The government overcomes this deficiency through a law dated March 23, 2014 passed through an accelerated procedure on January 20, 2014 by the Senate, on February 11, 2014 by the National Assembly and on February 18, 2014 by the joint committee.

Article 20 of the military planning law fits into the safe current, even if guarantees exist. The opinion of the CNCIS, unlike what happens for security interceptions, is not given *a priori*, but *a posteriori*. And the issue of time is discussed. On the contrary, the delays that accompany the notice are eagerly discussed. The authorization decision is transmitted in a 48-h delay to the President of the CNCIS. If the president considers that the legality of the authorization is uncertain, he takes the initiative of gathering the Commission.

Article 20 of the military planning law leaves judiciary questions in suspense, particularly that one in regard to the constitutionality of the law, as the constitutional council has not been addressed.

The decree from December 24, 2014 does not insist on geolocation any longer; it does, however, insist with regard to the connection data and the necessary evolution of technologies.

D) *Since 2013/2014, projects are studied in order to expand the possibilities of interceptions*. In July 2015[45], the law on intelligence came into force, passed in an accelerated procedure. This law expands the possible reasons for surveillance as follows:

– national independence, integrity of territory, national defense (existing reason);

44 CEDH, ruling Uzun C. Germany, September 2, 2010.
45 Law 2015.912 from July 24, 2015.

– major interests in foreign policy, implementation of international commitments, prevention of all forms of foreign interference[46] (new reason);

– major economic or scientific interests (existing reason);

– terrorism prevention (existing reason), infringements to the republican form of government (concept disputed by a certain number of jurists and members of the Parliament, new reason) and the stability of institutions;

– the reconstruction or maintenance of dissolved groups (existing reason);

– the prevention of criminality and organized crime (existing reason);

– prevention of the proliferation of weapons of massive destruction (new reason, in accordance to a certain geo-political context);

– prevention of collective violence capable of undermining public peace (new reason, sufficiently disputed).

Interceptions have become a common practice and are not at all used in exceptional cases to achieve the manifestation of the truth. The duration of the conservation of recordings is enhanced from 10 to 30 days. When data are encrypted, the delay starts from decryption. When the information contains elements of cyber attacks, the decrypted information is retained for months. The retention of records of implementation is modified consistently. The recording of content leads to metadata recording.

The law from December 12, 2005 and the law from March 14, 2011 involved the judiciary section. Nowadays, intelligence services can capture, set and transmit the words and images held in a secret manner, the computer data that transits or is held in a system.

Among operators, IPS, hosting providers, it has become possible, using an algorithm to intercept the information and install black boxes. Hosting providers, ISPs, operators are not able to refuse this cooperation with intelligence services. Anonymity may be imposed through authorization of the Prime Minister.

For mobiles, the IMSI Catcher, a false “repeater antenna” captures data transmitted between the electronic device and the true repeater antenna. The

46 Must align them with the reinstatement by France of military bodies integrated by NATO and the French military interventions mainly on African operations, foreign interference may consist of a cyber attack.

access of documents and information through the use of an IMSI Catcher allows the introduction of mass surveillance.

The authorization is issued by the Prime Minister for 4 months, and can be renewed.

E) *Guarantees appear with the National Control Commission of technical intelligence*,[47] *which takes over the CNCIS*. The Commission nationale de contrôle des techniques de renseignement (National Control Commission for information Technology) (CNCTR) encompasses magistrates and members of the Parliament and the President of the CNCTR is a judge. The independent administrative authority exercises control over all stages of interception executions.

In case of a breach of law rules, the litigation division of the State Council is consulted.

This law has been denounced by all defense agencies of human rights, by IPS, hosting providers, the Defender of Rights, Jacques Toubon (the latter had participated in the 1991 Act). Reservations were expressed by the CNIL, the last president of the CNCIS, the Union of Magistrates, the Consultative Commission on Human Rights.

In all the major Western countries, mass surveillance has a legal basis and its actors are both multinational Internet companies, mostly belonging to American capitals, and States that are able to install satellites over several continents.

The interceptions coexist with other means of social control. Such is the case of biometrics in the 21st Century, which develops improved or new applications with industrial competition of research laboratories.

47 CNCTR.

7

Other Methods of Surveillance

7.1. Biometrics

Biometrics pose a particular threat to freedom of movement. For Monique Chemillier-Gendreau, the notion of freedom of movement is "the idea of a common public good at an international level". It is important to establish a balance between the freedom of movement and the right of control through visas and passports of each State, under the principle of proportionality, intended to pursue travelers and migrants.

I) *The United States opts for a security regulation through visas and passports*

A) *According to Section 403 of the Patriot Act, the Ministry of Justice and the Ministry of Internal Affairs should work, with the support of the National Institute of Standards and Technology, in the development of technologies, which will be used to identify visa applicants and the people entering U.S. territory*. The chosen technology should be identical across every jurisdiction in order to facilitate exchanges. Section 405 requires the Minister of Justice to perform a report with regard of the FBI's digital fingerprint system. This report is also the evaluation about the systems that are used in other federal jurisdictions. According to section 414, biometric identification mechanisms are set into place no only inside airports, but also in ports and all points of entry of the American territory. The cost of this policy is high to the extent that the manufacturing of

Security and Privacy in the Digital Era, First Edition. Claudine Guerrier.

instruments geared toward the reading of documents incorporating biometric data is necessary.

The law of 2002 in relation to the enforcement of frontier security when entering the territory[1] is subject to the visa exemption of the countries, which are U.S. allies and hold a passport. Then, it is important to differentiate two types of passports: the machine readable passport as from October 26, 2004 and the passport based on biometric data as from October 26, 2005 to October 26, 2006. The United States pays particularly close attention to digital photos[2].

B) *In the context of US-VISIT, foreign visitors traveling to the United States with a visa are subject to submit, upon arrival at an airport or seaport, to a capture through a scanner of their fingerprints of the two index fingers* and having their digital photograph taken. Since 30 September 2004, these procedures also apply to visitors benefiting from the visa exemption program. According to American authorities, it is not a matter of undermining the freedom of movement. The US-VISIT program is therefore supposed to facilitate the freedom of movement (the authorities) or adversely affect such freedom (human rights associations).

C) *Concerning passports, the State Department chose the insertion of a radio frequency chip in order to reinforce border controls and institute a fight against false documents*. It opened the process of soliciting proposals from four contractors: the German Infineon Technologies, the American BearingPoint, the French Axalto and the Israeli SuperCom. The passport includes a Radio frequency Identification (RFID) chip, a radio identifier and, in the domain of biometrics, facial recognition. The chip, of a very low thickness, is included in the passport cover. Equipped with a memory capacity of 65 KB, it stores data, name, date and place of birth as well as a digital photo. When a person shows up to customs with the document, the information is transmitted once again to the control officer because of a scanner situated nearby. Since Spring 2005, these passports have been presented to the general public. In 2006, all passports were equipped with a RFID chip. The latter is relatively expensive, of course the chip includes a

1 Enhanced Security Border and Visa Entry Act.

2 "We will not change the deadline for digital photos" declared Michaem Chertoff, American Secretary of Homeland Security, during a G8 meeting in Sheffield.

digital signature and encryption technology, which increases the cost of a conventional Radio Frequency Identification System (RFIS).

Furthermore, the Ministry of Foreign Affairs and the National Security decided to set up facial recognition systems at airport customs stations. This program allows a comparison between the face of a physical person and the information contained in the RFID chip to be established.

The State Department wished to include other biometric data, such as fingerprints or footprints, but continuity was not given to this project as it would involve taking impressions of the whole population.

Associations engaged in defending individual liberties, including the defense of freedom of movement, are against passports with an RFID chip. In effect, the content can be read through clothing and at a long distance; under these conditions, stealing personal data is possible. Many associations such as the American Civil Liberties Union and Privacy International have sent a petition to the ONU, expressing their concern for freedom protection. Certain security specialists[3] demand the renunciation of RFID technology and the adoption of a chip that is in direct contact with a scanner. The choice of the RFID chip may induce malfunctions, even for criminal purposes, such as clandestine access to the information contained in the passports.

This restriction of the freedom of movement extends throughout the American continent. Prior to the Patriot Act, nationals of the American content were able to move freely to the United States. Since then, citizens of Canada and Mexico are required to present a passport or "another accepted document" to travel to the United States. Travelers by plane and that come from Mexico, Canada or Bermuda are required to present to American authorities a passport or any other accepted document. As of December 31, 2007, people coming from the West Indies and entering the United States by plane, by boat or by road, are also subject to the requirements that have been just mentioned.

D) "*Another accepter document*" is a secure travel card. It is no longer allowed for nationals from Canada and Mexico to enter U.S. territory with a

3 See: Bruce Schneier, founder of the company Counterplane Internet Security.

simple driver's license. Finally, adults from Canada or Mexico with children to whom they are not related to must prove that they hold custody of the children and show a letter from the parents or legal guardians authorizing the children to leave the country.

On the basis of the reform of illegal immigration[4] and in sensitive Mexican-American areas, the biometric card border crossing is mandatory since October 1, 2002.

II) *The European Union has widely followed the guidelines of American politics*.

A) *European citizens move and stay freely within the Schengen Space. Nonetheless, security measures have been strengthened between the signatory states. The Schengen Information System (SIS) is in place*. The SIS is a common database, an interconnection of national files containing information that remains national[5]. This database comprises more than 10 million records. Individuals whose data appears are the following: natural persons sought for extradition, nationals from third countries not eligible to enter national territory, missing persons, for example runaway minors or kidnapped ones. The second-generation SIS is installed. It takes into account the increase in the flow of information to control over people entering the Schengen zone to integrate into the central database of fingerprint facial recognition techniques and iris of the eyes. The individual freedom advocates perceive danger[6]. The SIS II expands it police function.

The Amsterdam treaty is a continuation of the Schengen agreement. It removes obstacles with regard to the movement of European citizens while fighting against the pathways of illegal immigration.

However, freedom of movement is minimized within the framework of the visa and passport policy.

Biometric visas allow us to exercise control.

4 Illegal Immigration reform and immigrant responsibility Act from 1996.
5 States may decide on their own whether to register in the database.
6 "The Sis will move on from a border control instrument of the European Union to a more 'proactive' tool of police investigation", Van Buuren, "The tentacles of the Schengen system", Diplomatic World, March 2003.

B) *To mark the occasion of the European Council of June 2003*[7], *the Heads of State and the government agreed to the introduction in 2005 of biometric data: fingerprints, irises in visas and passports*. The European Commission was already in charge of a study related to the development of an information system about visas[8]. It advocates retaining two biometric elements in order to identify individuals and better secure resident permits and visas. The choice fell through on facial recognition, which must be digitized and stored on a smart card inserted in the identification documents and on digital print. The European Union adopts a similar approach to American guidelines.

This position is criticized by human rights advocacy organizations and non-governmental organizations. For example, Statewatch, NGO based in London expresses its opposition: "The decision, by the European Council, to establish widespread surveillance of the movement of people was taken without any public consultation or any debate at the Parliament", according to Tony Bunyan, Director of Statewatch. He also states: "These proposals are just another consequence of the war against terrorism that shows that the European Union finds it equally important as the U.S. to establish mass surveillance systems, having more to do with political and social control than with the fight against terrorism".

C) *In 2004, a proposed regulation makes it compulsory to fingerprint*. This text is consequential to the meeting of the European Council of Ministers of Interior and Justice, which introduces adding fingerprints in a second biometric identifier for travel documents issued by the member States to their own citizens and residents. The majority of groups of Presidents of the European Parliament considered that there was not a change sufficiently important enough to bring to a review by the Commission of Freedoms and Rights of the citizens of the European Parliament. In case of refusal by the Presidents of the groups, the council was ready to take on an emergency procedure. The document was passed by 471 votes in favor, 118 against and six abstentions, with several amendments to the original text. All the Members of the European Parliament said that only one biometric identification was necessary[9], while permitting the

7 Meetings of June 19 and 20, 2003.
8 VIS.
9 Photograph.

different Member States to add fingerprints, if they wish and if they deem it necessary. The Greens have stated their opposition on the grounds of the principle of liberty and the principle of security. In their amendments, MEPs argued that there should not exist a central database of European passports to the extent that it could constitute a violation of the purpose, the principle of proportionality and that this could increase the risk of these data being used for purposes other than those for which they were originally intended. Certain MEPs also wished that the biometric information was used only for the authenticity of the document and the identity of the carrier and that the persons authorized to access such type of data were clearly designated in the regulations.

The latter is definitely adopted by the council[10]. Before, the group article 29, which includes the national bodies with regard to personal data, had wished that more guarantees were implemented, notably the assurance that biometric data would not be stored in a central database.

In fact, the regulation responds, first, to the will of Member States to improve the security of travel documents by inserting biometrics on the other hand, the will of the USA that require travel documents citizens of States that can enter the US without a visa.

The technology in travel documentation readable by machines is called Machine Readable Travel Documents (MRTD). Each type of MRTD contains, in a standard format, the details of the identity of the holder, a photograph or a digital image. MRTDs include machine-readable passports[11], machine-readable visas[12] and machine-readable official travel documentation[13].

The MRTS are made by the Advisory Group with regard to travel documentation of the International Civil Aviation Organization (ICAO); this group establishes and adopts specifications, which result in detailed technical requirements. Indeed, the OACI recognized the importance of the development of machine-readable passports and visas and therefore

10 2252/2004 Regulation from December 13, 2004.
11 MRP.
12 MRV.
13 TD.

recommended that the States issue machine-readable passports and visas according to the format presented in document 9303, normalize personal identification data included in travel documents to bring them into accordance with the details and recommended presentation in document 9303.

Human rights organizations[14] demand the European Parliament to reject the regulation because it establishes standards for integrated biometric elements in travel documents.

The Parliament did not follow these recommendations. On the contrary, the suggestions of the G29 with regard to the confidentiality, integrity and authenticity of data were taken into account. In fact, the contactless chip that contains the individual photography must have an electronic signature system that guarantees data authenticity and its integrity; these data should be encrypted so they are unable to be ready by just anyone.

The European Commission is studying the integration of biometric information in visas which should be issued by the member States. It considers it appropriate to combat document fraud that facilitates illegal immigration, human trafficking and terrorism. European Union visas are intended to be biometric.

On July 4, 2005, in Evian, the Ministers of the Interior of G5 expressed their intention of harmonizing the biometric data inserted in the official identity documents. The five states are planning to define common standards that allow interoperability and national identity cards[15]. The interior ministers also plan to extend biometric standards for driver's licenses, which are subject to multiple falsifications. They pointed out that harmonization would make it possible to provide administrative services online.

D) *The European Union, as a whole, tends to generalize biometric passports. On the deadline of June 28, 2009, the Member States should issue passports containing two digital fingerprints*. Germany offers the image of a pioneering state in terms of biometric passports, which is also true for the United Kingdom, but at a more modest pace than in Germany.

14 Such as Statewatch, Privacy International, IRIs in France.
15 They agreed to hold the fingerprint of the same finger.

The price of biometric passports is increasing consistently, but it is the security requirements that create the most problems. The security specialist, Riscure, was able to prove that the Dutch passport was unreliable by breaking security codes. Yet, the formula used in the United Kingdom was then very close to the one that existed in the Netherlands. In a general matter, biometric passports with RFID chips are often criticized in Europe, just like in the United States, due to a certain degree of uncertainty in the field of security. Thus, the Future of Identity in the Information Society (FIDIS)[16], which regroups universities, research centers and commercial European companies, issued a manifesto to the governments and industrial companies in order to draw attention about the flaws of the system. The FIDIS demonstrates that biometric RFID passports induce risks for the protection of privacy of users and are susceptible to generate identity thefts.

Certain passports are equipped with additional locks. For example, the American passport includes, in its coverage, a web of metal fiber. Two researchers[17] were able to demonstrate that a simple opening of half an inch was enough to intercept at a distance of 60 cm (2 feet).

The FIDIS also emphasizes the irrevocable nature of biometric data and the validity of 10 years for passports. These characteristics allow the fraudulent use of stolen data during a considerable period of time. Passports are exposed to interceptions, to “brute-force attacks”, theft of keys, cloning of RFID tags and improper use of remote reading. Based on its research, the FIDIS drafted several recommendations, corrective, in general, after the introduction of passports. It requests not to extend their use for authentication in the private sector, to inform citizens about the risks, to implement procedures to use in case of identity theft, to set up a prevention policy about the improper use of data contained in the passport and, in a more general manner, in all travel documents.

In the long run, the FDIS advocates the introduction of proven security measures for passports, more reliable than those proposed until now and debated choices largely between security experts.

16 Future of the identity in the Information Society.
17 Mr. Mahaffey and Mr. Hering.

European passports standardize the rules in the matter of biometrics, while limiting the freedom of movement. As an illustration, the example of France can be provided.

III) *France*

A) *A decree on November 25, 2004 authorizes the creation, on an experimental basis, and for the duration of 2 years, of a database recording fingerprints and the digitized photograph of people applying for a visa in seven consular offices*[18] and the registration of this data in an electronic chip associated with the issued visa. Consulted on this text, the CNIL ruled on October 5, 2004 about this experiment. If the registration of fingerprints in an electronic chip affixed to the visa raises no fundamental difficulties provided that the appropriate security measures are followed, in contrast the conditions of realization of experimentation especially as regards the formation of the centralized database provoked several reservations and objections.

The CNIL has thus considered that the creation of a file containing biometric data of people who have been granted a visa could be admitted on an experimental basis to the proposed framework, either for purposes of comparison, or on the condition that the requirements of implementation, consulting, supply, updating and deletion of the database are strictly defined. Such a file cannot be sustained in long term without having the CNIL entirely informed of its advantages and disadvantages, particularly, in the field of protection of personal data.

However, the CNIL estimated that given the objective of border control, the conservation of the file and the biometric data of people who had opposing views, a visa refusal was not justified; in fact, for those who presented themselves at the border, without a visa, consulting the central file would only confirm the absence of visas.

The decree on November 25, 2004 only partially takes on the observations and recommendations of the CNIL. Certainly, in accordance to its request, the purpose of this experiment was clarified and the device needs to be subject to an evaluation.

18 Bamako, Colombo, Shanghai, San Francisco, Annaba, Geneva, Minsk.

The decree stipulates that processed information will not be retained beyond the end of the experiment; however, the device relies on a central database in which the fingerprints of all visa applicants are stored, whether or not they obtained the visa. The criteria used for experimentation purposes are the following: importance of the flow of visa applicants, population size, territorial extension, number of border crossings by air, land or sea, capacity of the embassy or the consulate to arrange the experience.

In an embassy, the visa applicant is photographed, then proceeds to fingerprint scanning of all 10 fingers. Special devices photograph without ink usage. The information received is sent electronically to the border crossings equipped with biometric systems. At the border crossing, air and border police request the holder of a biometric visa to place the index finger on a device that reads its fingerprint. The police officer is also able to determine if the fingerprint is in accordance to the one that has been transferred by the visa services of the embassy. The counters equipped of readers are marked with a green dot. At the end of the experiment and based on the results[19], taking biometric data was widespread in 2007. A parliamentary committee of inquiry performed the review on biometric vista and experimentation[20]. In this point, the financial aspect is essential. The Ministry of Foreign Affairs and the Ministry of Interior need sources of funding. The Directorate of French People Abroad and Foreigners in France in the Ministry of Foreign Affairs insists on this point. Indeed, the extra cost related to the introduction of biometrics could be outweighed at a medium term by supplementary revenue. Certain people have proposed the creation of a support fund. This solution was not passed.

The inquiry commission supports Biodev and is opposed to a suspension of experimentation. The second phase is essential since it focused on several of the states from which illegal immigration emanates. Thus, all consulates have equipment to provide biometric visas in 2008. The sense of urgency is not identical. Priority is given to the country where migratory pressure is strong and the rate of fraud to the civil status is high.

Finally, the law of November 26, 2003, relating to immigration, uses biometrics. This usage corresponds, at first, on occasion of the debates, to articles 4 and 5, then, on its final version, to article 11.

19 With regard to this point, a study was made.
20 Biodev.

The law provides a file that lists the fingerprints of anyone applying for asylum or who obtains a visa for France. The draft legislation anticipated the statement, storage and automated processing of a digital photograph and fingerprints of all nationals from outside the community discharged when crossing a border of the Schengen area. This group of people is additional to that already foreseen by the Debré law: residence permit seekers, people in irregular situations or subject to expulsion measures from French territory. Approved by the Juppé government, this measure was not entered into force due to technical reasons. The bill anticipated an identical device for visa applicants. The latter are suspected to be in bad faith. What appeared in the statements of the Minister of Interior during the debates in the Senate is that it was in order to prevent fraud[21]. Furthermore, the policies seem to mistrust certain immigrants.

Before the National Assembly, the national bill was hardened. It did not take into account at the beginning the fingerprints of illegal immigrants or those who did not meet the entry requirements. Amendment No. 343 adds a digital photography to the fingerprints. Amendment No. 365 was also voted, which made systematic the recording of fingerprints. On the contrary, the law Commission rejected hostile amendments with regard to either the use or systematic use of biometric procedures. Certain senators defended that it is inappropriate to use biometrics in this context. Taking fingerprints is expected for those seeking a visa. However, visa applicants are not all criminals. The systematic filing can be considered an infringement to freedom[22].

Nonetheless, the political class in its majority is in favor of the file, arguing that French citizens that request a national identity card are required to record their fingerprints. However, the agreement is not ready. Socialist senators are in agreement with the fingerprinting of foreigners who obtain a visa and not for those seeking a visa. The problem of the practical implementation of fingerprint identification in consulate records is noted by all political organizations.

---

21 “Some people lose their visa or tear it after three months and then forget where they come from. This new file will constitute a special human aid to those who have lost their memory”. Nicolas Sarkozy, Senate, October of 2003.

22 “This helps to discredit all legal immigrants in France”, Nicole Borvo, Senate, session of October 9, 2003.

The law of November 26, 2003 must be in accordance with the provisions related to the protection of personal information. A decree in the State Council is passed after the suggestion of the CNIL, dated October 5, 2004. This decree holds the date of November 25, 2004. Personal data notably includes the digital photographs and fingerprints of visa applicants. Access rights and rectification are exercised at the Ministry of Foreign Affairs or at the consulate where the visa application was filed. In order to facilitate the authentication of the visa holder at border crossings, an electronic component is provided, which contains scanned images of fingerprints and the photograph of the visa holder, often associated with the visa sticker. Three series of provisions are executed by certain parliamentarians: the removal of the issuance of a residence permit a person who ordinarily resides in France after 10 years, the provisions related to family reunification and the jurisdictional procedure applicable to deportation measures.

On the removal of the automatic issuance of a residence permit, the Constitutional Council reminds of the prerogatives of the State: "No principle nor any constitutional rule ensures to foreigners rights of general nature and absolute access and residence in the national territory". "Only specific constitutional requirements such as the right to seek asylum or the right to lead a normal family life can obstruct the legislature's power to review, in a more restrictive sense, the right of residence of foreigners". In family reunification matters, the Constitutional Council considers that the new provisions are not against the rights of foreigners living in a stable and regular manner in France in order to lead a normal family life, which is guaranteed by human rights. It is up to the legislator to fix the period after which the applicant will be recognized as a resident in France in a stable manner. The 18-month period is not deemed excessive. It is also possible to deny family reunification when the applicant does not comply with the fundamental principles recognized by the laws of the Republic[23].

B) *A bylaw dated December 19, 2006 was finally implemented in accordance with article 7 of the law on January 23, 2006. It creates, on an*

23 These principles are "monogamy, equality between men and women, respect for the physical integrity of children and adolescents, respect for freedom of marriage, school attendance, respect for ethnic and religious differences, the acceptance of the rule that France is a secular republic".

experimental basis, an automated processing system of personal data with regard to the passengers recorded in the departure control systems of air carriers.

The execution of this automated processing system of personal data falls within the Police Central Directorate at the borders of the Ministry of the Interior. A decision of the Ministry of the Interior, communicated by the CNIL, specifies the origins and the destinations of the passengers located in the States that do not belong to the European Union. This personal information includes the number and type of document used, nationality, first and last name, birth date, gender, the board checkpoint used to enter French territory, or exit it, transportation code, which means the flight number and the code of the air carrier, time of arrival and departure, point of boarding and disembarking, the mention "known" or "unknown", which is kept during 24 h. The specific date for the fight against illegal immigration can only be consulted after 24 h after their transmission. The automatic processing is subject to an interconnection with the file of wanted people and the SIS. The right of access is direct: the data controller is the central management of the Border Police, attached to the Ministry of Interior. As for the data relating to the mentions "known" or "unknown" in the file of wanted individuals and in the SIS, the right of access is indirect, which involves the referral of the CNIL.

7.2. Passenger name record

Security laws are accompanied by the establishment of passenger name record (PNR) data in many Western countries. This implies a collaboration between air carriers and the authorities of certain States.

The International Civil Aviation Organization has longstanding worries about the "passenger name record". Air carriers collect information about the passengers as part of the booking services, then exchange it between intervening companies at the time of booking until the performance of the services requested by the passengers. The data that are present in these databases is standardized information recorded on an international level called "PNR". The PNR contains, depending on the services provided by the companies and requested by the client, specific pointers: the name and surname of the client, the information with regard to the travel agency where

the client's reservation was made, travel itinerary, elements comprising the flights: number of successive flights, time, hours, class, the group of people for which the reservation was made, an emergency contact of the passenger, electronic and telephone information, accepted rates, the state of the payment made and its modalities through credit card, hotel or car reservations on arrival, requested services on board: seat number requested in advance, meal information and the services brought up by the health status. It is uncommon for all fields to be filled out.

I) *Data from PNR should not be confused with APIS data*[24], which are collected by companies in the phase of registering passengers for a flight. They encompass the number and type of travel document used, the nationality, the complete name, date of birth, the border checkpoint used to enter in the territory of member States, transportation code, the departure and arrival times of the carrier, the total number of people transported and the initial embarkation point. There is less APIS data than PNR data. Nonetheless, APIS data are interesting as far as having them verified by the transportation personnel upon flight registration. The travelers provide PNR data at the time of the commercial reservation, which can change up until embarking. The PNR comes into force at the beginning of the twenty-first Century. The U.S., Australia and Canada establish "PNR Systems", which give place to interstate agreements. On November 19, 2001, the United States adopted a law on aviation and transportation security[25], on May 5, 2002, a law stipulated than from March 5, 2003 forward, air carriers should communicate to customs services and American security services personal data related to their passengers, under penalty of tighter controls, fines and even suspension of the right to land. These provisions include physical traveling persons and legal entities, which are airline companies and American security services. The Terrorism Information Awareness had as an objective to establish connections between police and judiciary information and the behaviors such as visa requests and the use of a credit card. The TIA was removed in September of 2003 and was replaced by the CAPPS[26] and the CAPPS 2, which applies, in the case of the latter, only for users of airline carriers.

24 Advance Passenger Information System.
25 The Aviation and Transportation Security Act.
26 Computer Assisted Passenger Prescreening System.

II) *Within the European Union, the United Kingdom is the only member State that has a complete PNR system in the framework of the e-borders program*. Coming into effect in March of 2008, this gathers, at the same time, the collection of APIS data and PNR data. The British system does not establish a distinction *a priori* between the flights entering from a Member State of the European Union or a third state.

III) *Australia and Canada have also put in place PNR systems*. Harmonization in the matter of protection of personal data has not ceased to create judiciary problems in connection to past agreements between States[27].

IV) *The U.S. request to the European Union to obtain full access to the PNR* of European companies. In May of 2004, the United States and the European Union signed the "2004 passenger name record data transfer agreement", which allows access to 34 details contained in the PNR. But American requirements collided with European rules in the matter of protection of personal data. The agreement was ruled invalid by the European Court of Justice[28].

A new agreement was completed on October 19, 2006 and entered into force on August 1, 2007. It is situated within the third European pillar, devoted to police questions and justice questions. The Parliament voted in disagreement, essentially due to breaches to the European right to personal data.

A next text was signed in 2012: in May 2010, the European Parliament delayed its vote on the PNR agreement with the United States. The Members of the European Parliament then invited the European Commission to negotiate a new agreement.

Legal practitioners have highlighted several questionable points of the agreement: PNR and extradition, period of use, sensitive data and data security and errors.

The reference to punishable extradition crimes do not fit in a PNR agreement because this notion applies only to suspects and not to people

27 This was the case in 2014 for PNR Canada/EU which was passed in 2011.
28 CJCE, Grand Chamber, May 30, 2006, European Parliament, European Union Council, Joined Cases C-317/04 and C-318/04 (the decision 2004/235 is excluded from the application scope from the directorate 95/46).

presumed innocent. The United States argues that because of the PNR, two "dangerous terrorists" were able to be stopped. Two terrorists in 10 years does not constitute a compelling statistic. Indian authorities were additionally outraged with the facility with which one of the "terrorists" had managed to take a plane so often between Pakistan, India and the United States.

The duration of use is well beyond the draft agreement[29] with Australia. This last agreement is deemed balanced. In the United States, the information retention period is undefined. It is true that the access to the data by the U.S. Department of Homeland Security should be progressively restricted. Nonetheless, data will not be erased. It is even possible to speak of the decline compared to the 2004 agreement only if the storage period is considered. Finally, Critics raised their voice against the reversibility of depersonalization. The agreement anticipates hiding PNR data after 6 months but it may be repersonalized by people with special access rights.

The agreement does not anticipate the immediate erasure of data considered "sensitive", contrary to the agreement from 2004. Thus, a food preference may indicate a religious affiliation. A hotel reservation or itinerary choice is susceptible to providing indications about sexual orientation. A medical request can allow finding out about a health status. Now, this sensitive data will not be erased in any case until after 30 days, if they fall within the scope of a specific investigation. So there is a potential risk of drift.

Regarding security, several countries including Germany, Austria and Belgium are concerned about the risks of data losses during transmission to third countries; appropriate technical measures and organization arrangements must be put in place in order to protect personal data contained in the PNR, accidents, destruction, losses, modifications, access, treatments or illegal uses. The protection, confidentiality and integrity of encrypted data, authorization procedures and documentation must be assured. Disciplinary sanctions are incurred in respect of anyone responsible for an incident in relation to private data.

V) *The PNR agreement at a European level seemed on the verge of being passed in January of 2015*. In fact, it is an agreement from December 4,

29 October 27, 2011.

2015 that anticipates a European PNR with 6-month conservation period of unmasked data[30]. It should be integrated into the legal corpus by 2016.

7.3. Data and files

The data are stored in files. Security files are essentially genetic files and police files. Two examples are taken into consideration: the United Kingdom and France.

I) *Legal sources*

At the Council level of Europe, two recommendations must be reported: recommendation R (87) 15 and recommendation R (92) 1.

Recommendation R (87) 15 tends to regulate the use of personal data in the police sector[31]; certain criteria appear in this recommendation: the delivery of a final decision, prescription, age of the involved party and particular categories of data. Recommendation R(92) 1 applies to the usage of deoxyribonucleic acid[32] in the context of criminal justice[33]: the information is deleted as soon as it is no longer indispensable to the initial purposes, when a judiciary decision has been taken; limitations to this principle are contemplated: databases are created when there is a conviction, when the conviction corresponds to serious offense, when the data retention period is indicated, when the conservation procedures are defined and when data retention is subject to a control or by the parliament or an independent body.

British and French examples are the means of lessons for genetic and police files.

II) *In the United Kingdom, genetic files gave rise to doctrinal analyses*. The United Kingdom is actually the only European State to allow the systematic conservation, and for an unlimited period, of DNA profiles and

30 The debate on the devation was rough.
31 Adopted 17 September 1987.
32 CONA.
33 Adopted 10 February 1992.

cellular samples of persons who have been acquitted or dropped. Does this mean that the principle of proportionality does not apply in the UK? The question is asked. The information in the profiles are objective. But the DNA profiles can be used and have, at times, been used in family research, which is questionable. Moreover, the files in the national police computer are accessible not only to the police but to bodies outside the police among which are legal persons of public law and private law, including BT, the Association of British insurers and certain employers. The computer is connected to the SIS. The United Kingdom considers that the preservation of the samples obeys to the ordinary legal principles governing the exercise of discretion and may be subject to judiciary control. The British Government argues, relying on statistics, that the samples and stored profiles represent an appropriate response to the fight against criminality.

The United Kingdom has taken the lead over other European countries in matters of scientific investigation techniques and, in particular, of DNA sample processing for the detection of criminal offenses. The other Member States of the Council of Europe have set limits to the conservation of samples and DNA profiles, while pursuing a legitimate aim in a democratic framework. A consensus was reached on the matter, but it was not shared by the United Kingdom, where the conservation does not have a time limitation. It is therefore possible to evoke an error of proportionality in terms of files in the United Kingdom.

III) *The situation is more complex in France.*

A) *In relation to the genetic files, the list of offenses where a genetic sample is possible is quite extensive*[34]. The refusal of genetic samples and genetic profiles on the occasion of one of these offenses is punished severely. It is considered an offense. In fact, it is rare for people to refuse genetic sampling and even rarer for people to be convicted based on the Article 706-56 of the Criminal Procedure Code. Sometimes, the genetic sampling refusal corresponds to trade union and political activism. Thus, members of the Confédération paysanne convicted due to having ripped

34 "Aujourd'hui, les trois quarts des affaires traitées dans les tribunaux peuvent entraîner un fichage génétique, à l'exception notable de la délinquance financière ou encore de l'alcoolisme au volant", declaration by Ollivier Joulin Syndicat de la magistrature, of the "*La justice simplifie le fichage génétique*" by Jean-Marie Manach, in "*Monde*" from July 3, 2007.

GMO plants generally refuse genetic sampling. Faced with this voluntary action, judge demonstrate a relative mildness, whose manifestation varies courts: thus, in Beziers, some accused of killing GMO plants was acquitted by the High Court[35] after refusing to comply with the procedure of providing a DNA sample. In Angers[36], the Court of Appeal upheld the conviction of a militant and established a fine of 200 euros for sampling refusal. This lady had been arrested after the destruction of transgenic corn in 2007. The magistrates confirmed the judgment of first instance was not illegal: this person was guilty of "damage to property". The debate is not over.

B) *It is possible to obtain the erasure of FNAEG data for accused people*[37] *and those who have committed one of the offenses mentioned in article 706-55 of the Criminal Procedure Code.*

These people directly address their request to the public prosecutor of the jurisdiction that handled the case. This erasure is considered "their preservation no longer appears necessary in view of the purpose of the file". The prosecutor communicates its decision to the applicant through a registered letter. If the prosecutor does not order the cancellation, the person in question may inform the judge of freedoms and detention, whose decision can be appealed to the chairman of the investigation chamber. When the judge of freedoms and detention orders the erasure, the prosecutor is able, too, to challenge that decision before the president of the investigation chamber. In both cases, the challenge is precedent for the execution of the decision. The French genetic file complies with the principle of proportionality: its conservation is not unlimited, its erasure can be considered and not all offenses are affected.

C) *Loppsi 2 was also interested in the files and two decrees in the Council of State were published in the French Official Gazette on May* 6[38] and 8, 2012. The relevant files on which the legislature leaned and the regulation is ruled are the handling of legal proceedings[39] and the serial

35 21 February 2009.
36 24 February 2009.
37 Section deux de l'article 706-54 du code de procédure pénale.
38 Decree no. 2012-652.
39 TAJ.

analysis file. The TAJ merged, as of late 2013, the STIC-processing system of infringements of the national police and the Judex, judiciary system of documentation and operation of the National Gendarmerie. This merger involves a significant work update, especially with regard to older data.

1) *The TAJ* is applicable to all people suspected of crimes, offenses and perpetrators of the most serious offenses. Storage and cross sensitive data can lead to malfunctions in terms of the protection of privacy.

Implementation and updating of TAJ-related software are controlled by a referent magistrate, who is a prosecutor. The TAJ retains data regarding the victims for a maximum duration of 15 years, and for a period of 5–40 years for the most serious offenses regarding suspects.

The Loppsi 2 law foresaw the establishment of a serial analysis file. Decree No. 2012-687 authorizes police investigators and the police to extract, compare and operate in a single file the whole environment of an offense, provided that it is punishable by a 5-year period of imprisonment.

2) *The serial analysis file* is able to use biometrics, since it is likely to use facial recognition with identification through photos. It is also coupled with the national video protection network. Finally, it can be analyzed and used for the data that feed links between individuals. In this way, the file is supplied with phone calls, but also with logs and all of the activities on social networks in the scope of the offense.

The software implementation is only allowed by the magistrate of the investigation or the judge of instruction. The specialization of the referent magistrate with regard to a background file and serial analysis will allow it to exert local or national controls on these treatments.

In terms of serial analysis files, the person in question is the person against whom there is serious or corroborating evidence making it likely that this person could have participated as author or accomplice in the perpetration of an offense mentioned in Article 230-12 of the criminal procedure code: the decree includes a large number of people being questioned. The notion lacks clarity, which is an element of legal uncertainty. A right of indirect access is provided despite the reservations of

the CNIL, who wanted the establishment of a right to direct access. As for the right of rectification, the decree does not indicate the modalities for exercising the right to rectify some people involved in the serial analysis files; victims and certain witnesses[40]. The CNIL stated that, in its view, the right to rectification was too vague and ambiguous. It felt that too much power was left to the prosecutor in an area that was in relation to individual freedoms. Nevertheless, the government has not followed the opinion of the CNIL, which it was not moreover required to do. However, the publication of notices and reserves of the CNIL allows any lawyer to easily pinpoint regulatory imperfections.

7.4. New technologies; geolocation, body scanners, drones are increasingly used

I) *Geolocation* is part of the current resources that are used by both companies as well as individuals. In the developed world and in emerging countries, geolocation concerns all public and private parties. If it is important economically, it also plays a mirroring effect in a judiciary plan. Indeed, the law has taken into account very quickly, in several branches, the issues of geolocation. The latter was subjected to a specific regime under the protection of personal data.

A) *The sources of law in the European Union: directive of July 12 2002, the directive of November 25 2009, the draft regulation adopted by the European Parliament in October 2013*.

Geolocation is particularly used in transportation. In social law, discussions were held with regard to the relationship between employees and location-based instruments to achieve traceability of employees by employers. In addition, geolocation is a key tool of intelligence. In various countries, people who are responsible for information by public authorities are questioning the status reserved for geolocation. For example, in France, in the context of the military program law of December 2013, the Senate has developed an article 13, which, at first, was vested in the geolocation practiced at the request of intelligence services, authorized by the Prime Minister along with security interceptions. Article 13 will experience an

40 In the sense of 3° from article 230-13 of the Penal Procedure Code.

evolution, since the law of December 18, 2013, with regard to the military program which applies not only to geolocation but also the connection data, and this at the demand not only the ministries of interior and defense, but also the economy and finance and budget ministries, for reasons relating to the breach of national security, crime prevention and crime, prevention of theft and criminality, the infringement of the essential elements of economic and scientific heritage of the country, the restoration or maintenance of dissolved groups. The authorization is issued for a period of 1 month. The CNIL regrets not having been able to express its views on certain points of article 13, now turned into article 30 of the law on December 18, 2013, but is being heard and will play its role during the decrees of the Council State that will allow the implementation of article 20. The Internet players[41] are showing their reserve because they fear an additional cost for the digital economy. As for the actors of the digital economy, they insisted on lobbying, but failed to put their views across.

The impact study [42] of the bill on geolocation distinguishes between two geolocation techniques in real time on the occasion of a criminal investigation: geolocation with dynamic following in real time, which is able, via an electronic communication terminal, to locate people and things, and geolocation with a dedicated device[43], installed over an object or transportation method, which allows us to determine, in real time, the location of an individual.

B) *Two judgments of the French Court of Cassation from October 22, 2013 led to a new law*: it is to substitute a magistrate for the prosecutor.

The public prosecutor, within the framework of investigations on which he or she has control, authorized real-time location-based measures in real time using an electronic communications terminal[44]. When the survey was finished and the judiciary information opened, the investigating judge also allowed real-time geolocation-based operations in a telecommunications terminal.

41 And notably the ASIC.
42 Etude d'impact afférente au projet de loi sur la géolocalisation, 20 December 2013.
43 I.e. tag.
44 Article 41, paragraph 1, of the Criminal Procedure Code, Article 60, paragraph 1 of the Criminal Procedure Code, Article 77-1-1 of the Criminal Procedure Code.

When real-time geolocation operations involve tag usage, they are, in most cases, used as a contribution to the investigation, which is not integrated into the procedure. However, the cassation court indicated that, during a criminal investigation, Article 81 of the Criminal Procedure Code allows the use of tags. Until 2013, real-time geolocation measures were authorized by the public prosecutor for investigation of in *flagrante delicto* and preliminaries by the investigating judge for the judiciary information.

The jurisprudence of the cassation court dated October 22, 2013 evolved the above-mentioned rules.

1) *Appeal 13-81945*

Mr. Mohamed X brought an initiative against the judgment of the investigating chamber of the Court of Appeal of Paris[45] on February 28, 2013. In an investigation conducted for a criminal association consisting of the preparation of terrorist acts, judiciary police officers, after having the authorization of the public prosecutor, asked electronic communications operators to locate mobile phones in real time, which were being used by Mr. X. Following an information discovery from the investigating judge of the Court TGI of Paris, new location-based measures of mobile phones were made based on a rogatory commission. Mr. X was arrested in his home, placed in custody, which was extended by the investigating judge of the TGI from Nantes; during police custody a search was conducted at the home of Mr. X in his presence. He was indicted on April 3, 2012 and Mr. X initiated an annulment action of the pleadings.

The means chosen is based on a direct violation of articles 6 and 8 of the European Convention of Human Rights Protection and Fundamental Freedoms, according to Articles 12, 14, 41, 77-1-1 and 593 of the criminal procedure code. A geolocation measure that tends to monitor the movements of a natural person by monitoring his/her mobile phone constitutes an interference in the private life of this person. No law convenes mobile phone surveillance. Articles 12, 41 and 14 of the criminal procedure code are general. Consequently, the investigating chamber has violated article eight, paragraph two of the European Convention of Human Rights Protection and

45 Cassation Court, crim, November 22, 2011, appeal No. 11-84308.

Fundamental Freedoms. A law cannot dictate the interference with the privacy of individuals only if placed in the execution, not under the orders of the prosecution, depending of authorities, but under the orders of judiciary authority, which presents guarantees of independence against public authorities. In this case, the investigatory chamber violated the text of the treaty. There is a partial cassation.

2) *Appeal 13-81949*[46]

Mr. Yohan Y launched a court action against the ruling of the investigation chamber of the Court of Appeal of Paris, dated March 5, 2013, and requested the annulment of the pleadings submitted due to infractions to the narcotics legislation. In a preliminary investigation, the public prosecutor had authorized police officers to demand electronic communication operators, real-time geolocation, which was called "dynamic monitoring" of mobile phones. An investigation was opened against Mr. Yohan Y, who was placed under investigation on March 17, 2012.

The legal requisitions aimed at geolocation involved the companies Bouygues Telecom and Deveryware. Geolocation and dynamic monitoring, authorized by the public prosecutor are in proportion to the seriousness of the committed or suspected offenses. These measures were also limited in time. Geolocation and dynamic monitoring constitute an interference that is not compatible with article 8 paragraph two of the European Convention for the Human Rights Protection and Fundamental Freedoms; articles 12, 14 and 41 of the French Criminal Procedure Code do not provide an adequate legal basis. The interference by the public authority in private life must be carried out not under the control of the public prosecutor, magistrate dependent from public authorities, but under the control of a court judge, independent of public authorities. In this regard, it is worth mentioning judgment G versus France[47] where it is mentioned that the judge of the public prosecution service is not an independent judiciary authority[48], and the public prosecutor has no standing in order to authorize location-based measures. The ruling violated articles 6 and 8 of the European Convention on Human Rights. The technique of geolocation is an interference of privacy, measure that requires the intervention of an independent judge due to its seriousness. The

46 Cassation Court, crim, Section 6, Mr. Yohan Y.
47 CEDH, G vs. France, November 23, 2010.
48 In the sense of Article 5§3 of the European Convention on Human Rights.

examining chamber disregarded the treaty text of the Council of Europe. Partial cassation is justified.

Under the law of October 22, 2013, the cassation court rules that a measure of real-time geolocation on a cell phone is an invasion of privacy. Based on this principle, the cassation court accepts the use of real-time geolocation when it is carried out under the supervision of an examining magistrate. When it comes to real-time geolocation operations in the context of a preliminary investigation under the control of the public prosecutor, the procedure is censored. The Directorate of Criminal Affairs and Pardons broadcasts on October 29, 2013, a telegram which draws lessons from this law. According to the analysis of DACG, if the case is related to the real-time geolocation of a mobile phone, the principle mentioned above applies equally to the geolocation performed with a dedicated device, in particular, a tag. The two forms of geolocation are intended to locate a person or an object. The judiciary sentence not only applies to preliminary inquiries, but also to flagrance surveys, research investigations into the causes of death, in the causes of disappearance or the search for someone on the run, all of which are led by the public prosecutor. Following the judgments on October 22, 2013, the French legal system is not likely to proceed with real-time geolocation in the context of investigations. Operations have been interrupted. On the contrary, geolocations investigated under the approval of an examining magistrate are carried out. The objective of the legislator is to establish a new system for operations that led to an interruption.

The law was passed in an accelerated procedure. In case of inquiry, the public prosecutor continues playing a role for a certain period; its length gives rise to a discussion before the two assemblies.

C) *According to the law of February 18, 2014, at the stage of the investigation, it is the prosecutor who, at first, issues an authorization for geolocation in real time*.

The quantum is debated before the National Assembly[49] and before the Senate[50]. The joint committee foresees that geolocation will fulfill the needs of an investigation or an instruction relating to a crime or an offense under

49 General threshold of 5 years' imprisonment and a 3-year threshold for crimes against persons.
50 Quantum of 5 years and 3 years.

Book II or under articles 434-6 and 434-7 of the Criminal Code, punishable by imprisonment of at least 3 years, of an investigation[51] or an instruction relating to a crime or an offense, with the exception of those mentioned in (1) of this Article, punished with imprisonment of at least 5 years.

For investigations of in *flagrante delicto*, preliminary inquiries, transactions are authorized by the public prosecutor for a period of 15 days; after this period, the authorizations are granted by the judge of freedoms and detention for a maximum renewable period of 1 month.

Exceptions to these procedures are provided in case of emergency leading to imminent risk of losing evidence or serious harm to persons or goods. Geolocation provisions may, in this case, be set up by a judiciary police officer who does not have the powers of a judge. The operations are then pursued by the public prosecutor or the examining magistrate within 24 h. If the emergency device involves being introduced into a living space, the officer gets in touch with the prosecutor who makes contact with the judge of freedoms and detention.

During the investigation, and if the operation is supposed to intervene outside normal working hours, authorization is issued by a written decision of the judge of freedoms and detention, delivered by the examining magistrate. In an emergency, if entry into a living space is necessary, the judiciary police officer must obtain the prior approval of the judge of freedoms and detention brought by the prosecutor; approval is given through any means and does not involve any written means.

This law was the subject of a consensus of the political class. The status of the judge of freedoms and detention tends to bend; this judge has more functions and he is more and more often called up to intervene.

With regard to geolocation, it tends to spread to the different stakeholders, businesses, public authorities and natural persons.

Among the technologies that play an increasingly important role, drones should be mentioned as well as dual-use technology, military and civilian.

51 Geolocation devices fall under investigation, for major countries, in 97% of cases.

II) *Drones*

The aerial transported drone plays an increasingly important role in the 21st Century, even if it existed before.

A comparative study will highlight the United States and France.

The drone was initially mostly developed in the United States, the world's main military power, and used in Pakistan and Afghanistan. The drone can kill without endangering the lives of soldiers.

France, engaged in several theaters of operations, particularly in Africa, has understood the importance of observation and surveillance drones. The military program law of December 18, 2013 focuses on surveillance drones while contemplating the establishment of a combat drone program. Regarding surveillance drones, tactical drones are used that allow permanent and accurate information, these are the *Système de drone tactique intérimaire* (interim tactical UAV system) (SDTI), which will be coming to obsolescence in 2017 and will be replaced by tons of vectors from here until 2019[52]. As for MALE drones, they participate in the "knowledge and anticipation" capacity. 12 MALE drones should be acquired by 2019. France has the intention to appeal to the American MQ-9 Reaper systems, via the Foreign Military Sale procedure, while being interested by French and European industry. Combat drones, in turn, are intended to replace combat aircraft, since they save the lives of soldiers. The option with regard to combat drones is European, which involves a privileged collaboration with the United Kingdom[53].

Second, civilian and commercial uses have multiplied, not only in the United States but also in most developed countries. In the spring of 2014, the European Commission announced proposals in order to develop the regulation of civilian drones in Europe: "… Many people, including myself, are concerned about the security, safety and protection of privacy posed by these devices"[54].

During 2014, the Commission conducted an impact assessment and the European Agency for Aviation Safety is at the source of security norms

52 With planned cooperation with the United Kingdom, another European military power.
53 With the United Kingdom, France also intends to work in the naval field in the system of fight against future landmines and carrier vessels called "mother ships".
54 Silm Kallas, Vice-President of the European Commission in charge of Transportation.

adapted to civilian drones, in view of "the gradual integration of RPAS[55] in airspace from 2016 onwards".

A) *Drones in the United States*

Drones, in their military function, appeared first in the United States. Military drones started to be used close to the end of the Vietnam War. In the private sector, drones constitute a primary source of digitization of personal data: because of the technologies that drones are equipped with[56], they contribute to the digital materialization of data that have a physical basis.

Indeed, images and other data that are collected and connected by drones then lead to its transfer and treatment over a computer and it is likely to end up, like any computer content would, stored on a machine or, in other circumstances, projected onto the network. An increase in the use of drones inevitably induces a collection of more voluminous data. This collection is facilitated by the air approach, which allows very wide scan areas to be overflown by the aircraft.

1) *In 2004, a NASA report[57] established a distinction between four categories of* "*mission*" *civilian drones:* commercial activities, Earth science[58], internal security and regional planning. Within the framework of these missions, many activities or disciplines are likely to use drones. The drone lobby is powerful in the United States. In particular, the Association of Unmanned Vehicle Systems International, which has worked hard so that the drones are allowed to circulate, should be mentioned.

On February 7, 2013, the Federal Aviation Administration provided a new list of drone approvals in the United States[59]. This list consisted of 20 approvals that brought the number of public bodies authorized to use drones to 81. These structures have different legal systems: they are the U.S. State Department, certain Sheriff offices in some counties, government agencies and universities.

55 Remotely piloted aircraft systems or drones.
56 Capturing of images, sounds and thermal information.
57 NASA, Civil UAV Capability Assessment, 2004.
58 Metherology, geology.
59 "FAA Releases New Drone List-Is Your Town on the Map?", EEF 07/02/2013.

From now until 2018, the commercial use of drones should see exponential development, reaching 7,500 civilian drones in circulation in the United States, according to the work done by the Federal Aviation Administration.

2) *Furthermore, police and intelligence services have envisaged devoting drones to surveillance*. Since 2014, border police have been using drone devices to limit illegal immigration. However, some U.S. states are trying to limit the use of surveillance drones so that no abuses are performed: 18 states were in favor of a limitation[60].

Drones have worked with video surveillance. In the United States, there are multiple intelligent video surveillance projects. TrapWire or INDECT should be mentioned, which use surveillance cameras, but also drones, armed, mostly, with biometric facial recognition technology, which can identify an individual according to size, age, gender and skin color. The drone can appear as a technological evolution that facilitates video surveillance on public roads. The camera is not fixed, it can capture several areas. It is a question of mobile video. The acceptance of surveillance drones poses the same political, sociological and legal questions as video protection. We must therefore take into account the possible factors of acceptance of video protection in order to transpose them into a board video system.

In the United States, associations for the protection of privacy, unobtrusive after the passage of the Patriot Act, militate not only for the illustration and defense of the First Amendment of the American Constitution, but also for the good application of the Fourth Amendment. The EPIC[61] and the EEF[62] work tirelessly in this direction and have focused on the difficulty of creating balance within the relations of "privacy" and drones. The Electronic Frontier Foundation has played a prominent role in the adoption of the Law on Freedom of Information, issued on July 4, 1966 under Lyndon Johnson, with inflections under Ronald Reagan and after the

60 "*States join battle over drone flights*", The hill, 17/02/2013, http//redirectrix; bulletins-electroniques.com

61 Electronic Privacy Information Center; Washington DC.

62 Electronic Frontier Foundation; Californian association dedicated to the defense of fundamental rights.

Patriot Act. With the appearance of drones, the EFF insisted on a necessary transparency toward citizens. The fight initiated late 2013 by the Democratic Senator Dianne Feinstein, who, nevertheless, usually defends the role of the NSA in life and intelligence[63] in favor of the reformed FISA law was quite widely publicized. Dianne Feinstein feels concerned about the increasing use of drones that could become systematic: "I have seen with my own eyes their surveillance capacity. There was a demonstration in front of my house, so I went to the window to look and see who was there, and there was a drone, there in front of my window, staring at me". Dianne Feinstein was heard in the Senate in December 2013 and brought a thoughtful testimony: "Evidently, the pilot was surprised because the drone spun and crashed. But was it equipped with a camera? A malicious person could have installed a gun on that drone?". The senator argued that the police must demand the systematic use of a warrant before any usage of a drone and also engage in a fact-finding mission when citizens are subject to surveillance through the means of one of these devices.

A concern of the same order is shared by a personality who does not belong to Dianne Feinstein's sphere of influence – Eric Schmidt[64]; he declared in 2009 with what could pass as legal flippancy: "if you do not want someone to be aware of some things that you do", the best is "maybe not do them". In 2014, Eric Schmidt manifested relative concern and called for the regulation of civilian drones. Indeed, he feared a situation where neighbors will be able to spy via drones, he also feared the use of drones by delinquents and criminals, including terrorists. "How would you feel it your neighbor went over and bought a commercial observation drone that they can launch from their back yard. It just flies over your house all day"[65] he said on 17 April 2013.

American police also has its reservations. According to the EFF, "Drones are capable of intercepting messages on Wi-Fi networks, tracking sixty-five people simultaneously, or identifying the brand of a milk carton from a height further than ten thousand meters?"[66].

63 Chair of the Committee of Intelligence of the U.S. Senate and supported the U.S. intervention in Iraq.
64 Google CEO at the time.
65 www.cnetfrance.fr; geeko.lesoir.be.
66 www.monde-diplomatique.fr/2013/12/PFLIMLIN/49974.

During these past few years, and notably, during the second half of 2013 and 2014, the majority of American states are interested in a thorough reflection on the regulation of the use of civilian drones in the American skies. The majority of laws that were eventually passed or are being passed involve obtaining a warrant to use drones for purposes of collection of personal data, but few of these laws have come into force.

3) *Complaints from American citizens in matters relating to drones are multiplying*. In the spring of 2014, the Capitol Hill Seattle Blog stated that a complaint was filed by a resident of Seattle. "This afternoon, a stranger was flying a drone over my garden and next to my house. I first took its loud buzzing for a lawn mower, due to this warm spring day, but I ended up looking through the window of the third floor just to see a drone, in a hovering flight, a few meters from here". This citizen added: "My husband went to speak to the owner, armed with a remote control, who was on the opposite sidewalk. He asked him to fly his drone elsewhere but the man replied that flying his drone next to our windows was legal". The plaintiff specified that the drone was armed with a photography device[67]. The man in question justified his behavior by saying he used his drone as part of "scientific research". This exception would be admissible if the man in question had been able to prove that he had accreditation, that he was using the drone for purposes provided by American law, which was not the case. Other complaints were then filed.

The courts have to decide with regard to home violations, and of course, on the infringement of privacy, the breach of the right to image and the undermining of the protection of personal data. Some American organizations focus on the temptation of technophobia. We must not allow, under the pretext of protection of personal data and the protection of privacy, that any interference is encouraged by the expansion of science and innovation required in various aspects of social life, both economically and legally.

B) *Drones in France*

Civil liability in France is based on articles 1382 and those that follow. The damage caused by a person must be subject to reparation. This also

67 With photographs, it is required to determine if there was any violation to the right of image.

applies to drones. The notion was echoed by the European Commission. If a drone has a malfunction and causes injury, it is important to determine who is responsible for dealing with the compensation: the driver, the owner or the manufacturer. Furthermore, it is important to know which eventual allocation rules and division of responsibility and liability limits apply. "The current civil insurance scheme was essentially designed for aircraft with flight crew and foresees that the bulk[68] determines the minimum amount of insurance".

1) *Two bylaws from April 11, 2012, which define requirements for various uses of drones, officially defined as* "*aircraft circulating with no one on board*" *and the constraints related to drivers*.

The first bylaw of April 11, 2012 is related "to the design of civil aircraft operating without people on board, the conditions of their use and the capacity of people who use them". The second bylaw of April 11, 2012 regarding "the use of airspace by aircrafts operating with no one on board". Article two stipulates: "A remotely piloted aircraft circulating with no one on board is said to evolve when flying away from the remote pilot as this individual retains a direct view of said aircraft allowing him to prevent collisions by applying the rules of the air". In other cases, this is referred to as "circulating out of sight". These users of Parrot drones and other lesser known brands are expected to master their machine and they undertake liability in the case of a civil accident, said the General Directorate of Civil Aviation. An agent of the public force is required to speak to an offender if he does not conform to the use of the bylaw. And if the drone harms a person, the other person is subject to penal sanctions.

A bylaw dated December 17, 2015, applicable after January 1, 2016, completes the regulations of recreational drone use in France. It is forbidden to use drones if there exists a risk to people or property on the ground, and also above public spaces in urban areas. The drone is required to fly at a height less than 150 m or 50 m in some areas of military maneuvers and training, listed on Dircam's site[69]. It is prohibited to pilot a drone from a car, a bicycle or any vehicle in motion. Drones should weigh a maximum of 2 kg, except for those that are piloted under sight.

68 From 500 kg onwards.
69 Directory of air military traffic.

2) *Drones for professional use which are intended, for example, to inspect art structures, fall under another regime.* These bylaws establish a regulation based on the categories of drones and the type of use for which there is recourse. Civilian drones are classified in various categories, from A to G. This classification varies with regard to the weight, type of propulsion and the nature of the activities involved. The obligations under this classification are based on the use of the aircraft: speed, flight height[70], type of area flown[71] and end goal.

Only Class A aircraft models[72], which circulate in direct view of their remote pilot, are exempted from navigation document and are allowed to fly without special conditions relating to the required capabilities of the user.

Nonetheless, the use of other categories of drones, in particular those equipped with cameras, is subject, according to the category of aircraft involved and the type of activity, to obtaining a permit, which is issued by the minister in charge of civil aviation as well as the installation of specific devices[73]. A minimum level of proficiency is required from the remote pilot and the possession of specific documents[74].

3) *In matters of accountability, the operator of an aircraft is responsible for the implementation of necessary measures to ensure the safety of third parties*. "The real concern is that in the field of cameras. The person may of course be limited to filming what is happening in the garden, but the machine can quickly climb over the fence and catch the neighbor while she's in the pool [WAR 11]".

Control is essential. Daniel Warfman establishes a comparison between drones and antiradars. Only the antiradars controlled in possession of the tool are able to be sanctioned. "Unlike fixed installations that can be easily controlled, temporary and mobile installations are generally undetectable. Image transmissions will be able to be pirated".

70 Visual flight by day or flight out of sight.
71 Populated area or not.
72 Less than 25 kg, one type of propulsion, no cameras.
73 Barometric sensor that enables the remote pilot to know the altitude or device "fail-crash" to allow a forced landing.
74 Operating and maintenance manuals, navigability documents, special activities manual.

Numerous French companies[75] exploit civil drones via operators. In March of 2014, over 430 operators were allowed to fly these engines in the French skies by the General Directorate for Civil Aviation: "Every month tons of additional players are added to the operators already present on the market"[76]. The most involved sectors in 2014–2015 are the supervision of works, such as the SNCF railways, precision agriculture, which tends to identify weak and strong surfaces to achieve an appropriate dosage of fertilizer, surveillance infrastructure such as pipelines or oil platforms and the making of stories by the media.

Entry into the market is regulated. In order to be an operator of civilian drones, four conditions must be met: to be approved as a company, to be accepted as a drone pilot[77], to have subscribed liability insurance and to have a drone certified by the General Directorate of Civil Aviation. If drones or their conditions of use do not meet the conditions set by the DGAC, operators are required to seek special permission from civil aviation, under threat of a penalty that can go up to €75,000 fine and a 1-year period of imprisonment.

If the bylaws from April 11, 2012 define a regulatory framework of reference for the use of drones, this further impacts the protection of people and property and their privacy. Other legal provisions must be observed. It is also appropriate to quote Article D133-10 of the civil aviation code that poses requirements that must be obeyed by people who carry out aerial photography, particularly using drones. This section prohibits "taking aerial views through camera, film or other sensor" of certain areas and requires prior notification and authorization for some images or data recording of the national territory.

C) *At a European Union level, the Commission intends to improve the protection of the privacy of people whose activities might be affected by drones* "The European Commission will examine how to ensure that data

75 See: RFF, EDF, SNCF, GRT Gaz, Veolia, Eiffage.

76 Emmanuel de Maistre, then President of the Professional Federation of Civil Drones and Director of the company Redbird.

77 There is currently no authorized education in France, that would be recognized, to perform this job.

protection rules are fully applied to remotely piloted aircrafts and will propose amendments or specific directions, as necessary"[78].

On safety, the Commission, very attentive to the economic development potential of drones, created a working group to publish a roadmap with regard to the secure integration as of 2016 onwards of civil drones in the European aviation system[79]. The Commission report develops the issues related to security and privacy. The Commission announced on the April 11, 2014 hearing the development of a regulation to normalize the use of remotely piloted aircraft systems. The regulation should apply to air safety, respect for privacy, and liability in case of an accident. The Commission gave its agreement to the ASEA[80] so that it is immediately able to "get on with the establishment of security standards". It should, at the same time, regulate the use of civilian drones and "ensure the gradual integration of the RPAS in airspace from 2016 onwards". And the Commission insists on the economic issues that civilian drones bring with them: "The project aims to enable the European industry to become a world market leader in this emerging technology". To do this, the Commission intends to "rationalize the work of R&D, including the funding of the European Union devoted to R&D managed by the company SESAR"[81]. However, these financial aspects should not hide the essential aspects that constitute privacy protection. On December 7, proposals were made to establish four action regimes of drone uses in the European Union: a regime of freedom for drones of common use, an authorization system for drones geared toward professional use, and two other authorization regimes for drones that have a higher weight.

The French CNIL, in October 2012[82], initiated a reflection on the ethical and legal frameworks to implement for drones and surveillance. "Home-made" drones or "toy-drones" are likely to be used by voyeur neighbors: "since it is equipped with a camera, a mobile camera, a sound sensor or even a geolocation device, a drone can potentially adversely affect privacy, capture, and disseminate personal data" explained the CNIL.

78 IP/14/384, April 8, 2014.
79 Press release of the European Commission of June 19, 2013 titled "Drones stimulate innovation and create jobs".
80 European Agency of Air Security.
81 Single European Sky.
82 Note from October 30, 2012.

Indeed, based on the mobile camera sensors, the camera, microphone, sound or heat sensor or device geolocation, videos or photos taken using these drones can achieve the recognition of facial features, morphology, a person's movements and read license plates. We can question the transposition of the obligations of the law of August 6, 1978, as amended by the law of August 6, 2004, in case of using a civilian drone. It seems almost impossible to systematically "blur" the faces of people filmed by a drone before the release of the film.

The law of January 6 1978, amended by the law of August 6, 2004, has provided specific treatments for video protection. If drones equipped with cameras are similar to surveillance systems, it is possible to question the application of the video surveillance/video protection regime. However, the transposition of these rules is complex. Who can use a drone filming the street and is empowered to view images captured by the drone? When a drone films public roads, how is it possible for people being filmed to be informed that such a system was put in place and oppose the capture of the image? Neither the doctrine nor the jurisprudence has yet found answers to these questions. Furthermore, the new regulation on the protection of personal data does not include any article on aircraft piloted remotely.

The legal provisions apply from the moment the image of people is recorded or viewed through a digital medium if it is not of a purely personal activity.

Nevertheless, the exponential increase in the use of civilian drones in the United States and Europe raises questions and concerns about civil liberties. The drones are inserted into an international dimension. On October 19, 2013, the special rapporteur on extrajudicial, summary or arbitrary executions and with regard to the promotion and protection of human rights and fundamental freedoms in the fight against terrorism[83] published their report on the use of drones under the fight against terrorism. According to the report by Ben Emmerson, there may be doubts about the so-called "low level" target. There is a disagreement here between the strict position of the CICR[84] and the defenders of American positions according to

83 United Nations.
84 International Committee of the Red Cross.

which a member of a terrorist organization can be targeted at any time. The exception introduced by the jurisprudence of Carolina of the U.S. Supreme Court must be interpreted strictly: the need for legitimate self-defense must be "immediate, compelling and should not leave choice of means nor time of deliberation"[85]. Beyond this military problem, the main issue at the moment is that of the civil drone, with the key issue of accountability and the protection of privacy. Should we fear a future "where drones would be used to monitor the comings and goings of everyone, by the police, by burglars, a nosy neighbor, in short, by anyone?"[86].

IV) *Finally, the body scanner is becoming widespread in airports, whether in the United States, within the EU, and notably France*.

A) *It is the United States who started the establishment of body scanners in most Western countries, within the framework of airports*. Certain States resist American pressure, however the majority of U.S. allies follow its example. Even within the United States, the body scanner provoked controversies due to medical and legal reasons.

In the medical field, studies have been conducted. They did not lead to definitive conclusions but they do feed fears in relation to cancer. Even scanners manufactured by L-3 Communications, which emit only low radiation scare numerous citizens. The U.S. government insists on the harmlessness of the whole body scanners installed in airports, but is fraught with mistrust of the persons concerned, sailors and passengers who are not convinced by the repeated guarantees from the FDA[87]. The scientist Peter Rez[88] claims that "the most disturbing is what might happen if the equipment does not work anymore and releases too much radiation". The risk is much higher than the one incurred with a medical scanner because airport scanners work more than medical scanners do and are used by employees of the Transportation Security Administration (TSA) who have received no medical training. Moreover, the Health Physic Society, a scientific association who works on the safety of radiation, reports that the profession

85 See: Report by Christopher Heyns: a drone attack can only be lawful if it meets "all applicable international legal regimes" (right of use of interstate force international humanitarian law); http://dommagescivils.worldpress.com/2013/.
86 Fabien Soyez, www.cnetfrance.fr/news/vieprivee_bientôt_des_drones_à_votre_fenêtre.
87 American Federation of Health.
88 Physics University of Arizona.

of a pilot has a higher risk of cancer than the population average. Many citizens would like to apply the precautionary principle in this area.

1) *A lot of Americans also believe that body scanners violate privacy. Tests were performed in 2002 in Florida*. A quarter of potential passengers refused to move toward the body scanner and opted preferably for the metal detector and body search.

2) *The body scanner reveals, only to the agents of the TSA, the utter privacy of those people stopped and many citizens fear that their naked photographs* will be found on the Internet. This fear has been exploited by companies and one of them has developed a new line of underwear that is supposed to block radiation and enforce privacy. American citizens can refuse the use of body scanners; however, they must then go through a thorough physical search that does not necessarily respect privacy more.

A body scanner boycott movement took place on the eve of Thanksgiving Day 2010. Thanksgiving was chosen because it corresponds to a day when Americans travel a lot and use airports. The slogan of the protest was: "Travel with dignity". Only one or two passengers refusing to use the body scanner was necessary for seriously delaying travel[89]. The right to privacy and private life, jeopardized by the body scanner, was echoed by multiple associations that defend human rights. Thus, EPIC filed a lawsuit to suspend the deployment of body scanners in U.S. airports because they would be "unlawful, invasive, ineffective"[90].

American authorities are urging European governments to strengthen security in air transportation and to introduce body scanners. The laws vary and take into account the relative economic, industrial and technological strength. The body scanner belongs to the kingdom of means but also to the kingdom of ends, in part.

B) *An experiment took place in France in the form of millimeter wave technology at Paris airport*; the first experiment attempted at Nice airport was abandoned following protests by a number of passengers and human

89 According to estimates, it would take 15 min to get 100 people through body scanner control but at least 6 h to submit the same number of people to body search.
90 http://epic.org/privacy/airtravel/backscatter.

rights organizations. Loppsi 2[91] legislated in France with regard to the body scanner.

The body scanner approved in France is the millimeter waves scanner due to health reasons. In fact, serious reservations are likely to be expressed with regard to the absence of dangerous waves emitted during inspections. No thorough impact assessment has been conducted on the safety of the devices that use X-rays in a non-medical environment. Only the millimeter wave scanner, in this context, is acceptable, although it has not proved its harmlessness.

The visualization of images produced by the body scanner can be revealed to be intrusive and detrimental to people's privacy. The French legislator was inspired by the advice of the G29.

Viewing of images is restricted to trained and qualified personnel in premises that are not open to the public. Those who proceed to control belong to the same kind as the passenger. These provisions had previously been introduced for rub down searches.

The CNIL emphasizes the necessary nature of training of operators which makes it imperative to protect privacy, and advocates limiting the retention of images to the essential duration of the control. It also recommends – but this point was not followed up – that viewing images is carried out in locations prohibited to the general public and is limited only to authorized persons.

Searches and visits are conducted with the consent of the controlled natural person. In case of refusal, the person is subject to another control device.

The analysis of viewed images is performed by operators who do not know the identity of individuals and who are not able to simultaneously visualize the individual and his/her image produced by the body scanner. The image must have a system that blurs or even prevents face recognition. The storage and recording of images are prohibited. In this way, there will be no identifiable database exploitation.

91 Law of March 14, 2011.

1) *Until January of 2011, the bill passed on first reading by the National Assembly and the Senate stated that an ordinance of the State Council should determine the airports and destinations for which the use of control by using imaging devices through millimeter waves is authorized*. The location of these airports is not indifferent because only one experimental location existed in 2011 and is dependent on Aéroports de Paris. The ordinance of the State Council is supposed to provide legal certainty to the question of the location of airports, which, at first, is restricted. The opportunity to use this appeal is questioned.

2) *A ministerial ruling is proposed through an amendment by Jacques Gautier*[92] "A joint ruling of the Minister of Civil Aviation and the Interior Minister determines the airports where the use of control through imaging device using millimeter waves is authorized". The ministerial ruling has an infralegal value to the ordinance of the State Council. The guarantee for individual freedoms is of lesser significance. On the other hand, the two ministers covered by this amendment are actually involved: the Minister of Civil Aviation is responsible for the activities of air terminals and their facilities; the Interior Minister is responsible for matters relating to national security. The ministerial ruling replaces the ruling of the State Council.

The experiment is scheduled to last 3 years, which corresponds to an almost irreversible commitment. Some criticism remains possible: anonymity is not fully guaranteed. The question was raised by the European controller of data protection, in his commentary relating to the communication[93] of the Commission of the European Parliament and the Council in relation to the use of security scanners at airports in the European Union. In order to keep anonymity of natural persons taking body scanners, two authorized people operate simultaneously: one of them brings the passenger in the scanner and the other looks carefully at the screen display and performs the corresponding control. The European Data Protection Supervisor states in the above-mentioned communication that anonymity cannot be guaranteed 100%. Even in the hypothesis where no direct connection is established between the authorized person who analyzes the images and the traveler who is subjected to the scanner, it remains a possibility of indirect identification since the authorized person can be in

92 Amendment no. 73 rectified, Senate, January 19, 2011.
93 2010 311 finale.

contact with other agents who could potentially identify the traveler. Yet, this is not at all impossible in an environment where identity cards and passengers' passports are handy for a number of individuals who are able to make a comparison with the photos in the identifications. Total anonymity cannot be proposed and it is a fact to remember because anonymity is desired by the passenger using millimeter wave body scanning.

Privacy is insufficiently guaranteed.

Loppsi 2 orders that for the body scanner, as well as for the physical search, the traveler is checked by a person of his or her gender. It would be a guarantee against the violation of the most intimate part of an individual. Some human rights organizations have noted that it was appropriate to take into account not only gender but sexual orientation of the person entitled to check. Yet, sexual tendencies belong, within the Directive Framework 95-46, to sensitive data and should not be the source of discrimination. In this context, it is almost impossible to question a future controller to determine their sexual orientation and whether it is possible to check a person of the same gender as him (or her). The Association européenne pour la défense des droits de l'homme (European association for the Defense of HumanRights) (AEDH)[94] notes that "…people are distinguished not only by gender but also by their sexual orientation. Will they have passengers declare their sexual orientation during the inspection? If we add to this the problems that a transsexual may face, it is in an impossible situation whatever the terms of use of the scanners, it cannot stop interfering in the personal life of an individual and violate personal data". So, it is particularly difficult to ensure that the privacy of a traveler does not suffer during use of the device in spite of the intrusive nature of the body scanner.

3) *Consent is also insufficiently guaranteed*

Consent is necessary for relying on the body scanner. In a country that respects human rights and the main international instruments in this matter, it is beyond question to subject force on someone in order to use the body scanner. This is why the refusal is integrated into Loppsi 2. This refusal is accompanied by an alternative: any traveler who does not want to use the body scanner through millimeter waves "accepts" a metal detector control

94 "Security scanners in the European Union", February 15, 2011.

and a body search. A passenger cannot refuse all forms of control; otherwise, he/she will be subject to penalties. Incidentally, the refusal of any control implies the inability to make the journey by airplane for which a reservation was granted.

Can we, in this context, talk about a free and informed consent? If the passenger has to choose between passing a scanner and another method of control, it must be determined whether this freedom of choice is real or if travelers are forced, implicitly, and not explicitly, to opt for the scanner. For example, if the refusal to be subjected to the inconveniences, real or imaginary, of the body scanner, induces denial of boarding by the airline, the contract initially planned is therefore not executed, so the choice does not exist and the issue of consent is biased: there is no possibility of materializing the agreement of wills between the parties, as mentioned at the beginning in a bilateral contract, since the transport service is no longer offered.

If the refusal of the scan results in a supplementary and long wait leading to the alternative control system, and if this additional wait can result in a delay so that the passenger, although he acquiesed to an alternative control method, is not able to board the plane for which he had taken out a reservation, the freedom of consent is partly biased. Indeed, the traveling contractor may be opposed to the use of body scanners, taking over everything in the contract, the materialization of entering into the foreseen time and date into the cabin to the chosen destination. In this case, the client may reconsider his/her refusal and accept the body scanner. Is this the case of an unbiased consent? Doubt is at least admissible.

Finally, the passenger can deny the body scan and be subject to an alternative solution, which is often a physical search. The passenger is able to consider the physical search as humiliating. He/she considers that the physical search is less intrusive than body scanners on individual freedoms but considers that the body search also infringes fundamental freedoms. In this context, the consent is not free; the legal act is not based on an agreement of informed will. Furthermore, it is possible for the airport to be inadequately equipped and may not have a private location where the physical search is conducted, away from the public eye. If this hypothesis is confirmed, the traveler is “exposed” to the public and guarantees for

protection of privacy and intimacy are not met. For AEDH, in this situation, "consent is not free, it is rather a biased consent obtained under coercion. The only alternative to the scanner does not exist in these conditions and the right to consent is infringed".

Yet, the new European regulation puts particular emphasis on personal data on the concept of consent.

As with Loppsi 2, it is evident that the body scanner is added to other security systems, SIS[95], VIS[96], Eurodac database, baggage screening and metal detection; the scanner completes a miscellaneous system of control techniques.

95 Schengen personal information files.
96 European visas.

PART 3

Between Security and Freedom

We are in the downward spiral of machinism as analyzed by Ellul. The new machines represent an issue for industries and microeconomics entering the circuit of supply and, demand, and, as such, are being partially legitimized. Certainly, the legislator is the regulator and can prohibit this flow of machinery but the mission of the legislator implies the intervention of the executive and the legislative. The executive and the legislative are interdependent with the other actors. The kingdom of means and the kingdom of ends coexist and intertwine. The body scanning machine belongs to the means because it is through the security scanner that security breaches, such as explosives, can be detected. It is more perfected than the metal detector: in the chain of machines, it comes after the metal detector, due to its temporality and its degree of complexity. Nonetheless, the body scanner also raises questions encompassing the kingdom of ends and ethics. The interference with privacy, which subsists, even if the image is not saved or stored, is well within the kingdom of ends. Belonging to the kingdom of ends has been stimulated by the United States, but the States of the European Union are becoming increasingly likely to participate in this security link; other countries, emerging ones, maybe developing ones, are affected by this insect related to mechanization: the kingdom of means/the kingdom of ends.

In this context, actors play a diversified role: corporations carry the product/machine, often with protection from patentability. However, products/machines are quickly obsolete and businesses design new products that seem, at first glance, sufficiently respectful of privacy (but this point remains a watermark). The States are committed to security and they tend to

Security and Privacy in the Digital Era, First Edition. Claudine Guerrier.

encourage the development of all products/machines that have some degree of efficiency and are connected to security requirements. The range of players seems to deliberately lean in favor of safety products/machines. Still, the kingdom of ends is not hidden.

In this 21st Century, where the main actors, States and multinational companies, are behind products/machines that are sources of profit, Jeremy Bentham's analysis seems to become reality. The panopticon is already here. Citizens are constantly surveilled and they do not appear to suffer in this respect[1]. They live to the drum of technologies of control and seem to join them, to some extent. Is this Big Brother? Not really, since users "accept" the cookies and profiling that follows, the interceptions, the behavioral and biological biometrics. Does this pseudo-adherence makes mass monitoring lawful? The question is being asked and concerns NGOs, who sometimes substitute for the representatives of the legislative, in order not to neglect the kingdom of ends.

Now, we have come into what can be called the "era of compromises". In this era of compromises, security omniscience continues to take a prominent position. Industries and companies continue to manufacture products/ machines that are able to track individuals in the various spaces of the time, the virtual and real.

Nonetheless, the kingdom of ends is never forgotten, even if it is a little biased. A legal or ethical reflection continues to be backed up by sociologists, jurists or law philosophers. So it happens that the jurisprudence takes into account certain facets of privacy or personal information. It appears that the law or the legislations are able to take into account what appeared to be a chip of human rights in their colorful connotations. Therefore, a difficult cohabitation exists between the continuous appearance of social control techniques and an ambivalent reflection with regard to the law, whether natural or utilitarian.

1 Common media catchphrase: "What fear do you have of being monitoring if you have nothing to hide…".

8

Towards Compromise

8.1. Legal measures have been taken in order to protect some fundamental freedoms

I) More and more frequently, when security measures are provided, regulatory authorities are expected to offer guarantees to natural persons.

A) *United Kingdom*

1) *Since the beginning of the 21st Century, the security Regulation of Investigatory Powers Act (RIPA) has adopted dispositions that want to be protective of liberties*: an ordinance of Home Secretary that imposes a capability of interception that must be presented to Parliament and must be approved by both chambers[1]. A communication service provider is entitled to dispute the obligation related to interception capability before a specialized court[2]. Protections are established. The principle of proportionality applies to the desired information and purpose of the request and the objective performed under the RIPA[3]. Furthermore, guarantees were introduced in RIPA: a commissioner (Interception of Communications Commissioner) monitors the exercise of powers granted to the designated people[4]. A court is in charge of receiving complaints from the public. The commissioner, an independent commissioner, a high-rank magistrate

1 Section 12(10).
2 Section 12 (5) and (6).
3 Section 22(5).
4 Article 57.

Security and Privacy in the Digital Era, First Edition. Claudine Guerrier.

appointed by the Prime Minister for a commission of 3 years, which can be renewed, assures internal control of the system by on the spot checking according to the relevant services, the application conditions of the legal provisions. All players involved in the execution of interceptions are expected to facilitate their work, transmitting the necessary documents and information to the investigations. The commissioner is required to make reports. It is convenient to establish a distinction between two types of reports. In the first case, if the commissioner finds breaches to the law, he or she writes a report in all the circumstances where it appears to be indispensable and sends the document to the Prime Minister[5]. The other type of report is the annual general report compiled from the conclusions drawn from the confrontation between theory and practice, and between the law and its application. This report is communicated to the House of Commons and House of Lords but the Prime Minister can refuse the publication of certain passages of the report to Parliament if he/she considers that the impugned sections are likely to harm national security, could affect preventing crime or safeguarding the economic potential of the United Kingdom.

2) *The second level of control corresponds to an independent court*[6] formed of five members, who have been granted a mandate of 5 years, which can be renewed, appointed by the Queen and all derived from the parliamentary majority. The members of this court have judiciary experience of at least 10 years. With regard to the powers of the court, they are not exhaustive. The court is appropriated by people who think that they are the subject of interception measures. In the investigation that he/she successfully attains, he/she is assisted by the commissioner, who, as part of his/her mission, is able to gather information that is useful to the court.

Following the investigation, the court has substantial authority. If it concludes that a violation of the law took place, it informs the applicant of that conclusion and reports to the Prime Minister of its investigation. Moreover, it can decide through an ordinance of the cancellation of the ministerial authorization, the destruction of minutes of proceedings and tapes containing information intercepted illegally. The court is also likely to set a compensation with regard to the damages and interests owed due to

5 The report had two parts, one was public and the other one secret.
6 Interception of Communication tribunal.

damages suffered or it can engage the competent minister to pay the plaintiff the amount of compensation assessed by the court.

The commissioner noted in one of his/her reports that in addition to the integrity of the services involved in the interception of correspondence, the measure of vital protection against possible abuse of the institution would be the trials attached to police services, customs and intelligence services acting as plaintiffs and the minister acting as an administrative service granting authorization and, ultimately, executive services.

In fact, if the reports communicated to Parliament were allowed to form an assessment of the political interceptions in the United Kingdom, individual trials were almost never successful. The record is mixed for this two-headed control institution. The legislative provisions of the fight against terrorism have not facilitated the action of the "Commissioner" and the independent court. Individual applicants, moreover, have not been satisfied.

B) *Sweden*

1) On June 18, 2008, the Swedish Parliament passed by a narrow majority[7] a law that authorizes a civilian organization, headed by the Ministry of Defense, in order to establish interceptions of electronic communications. The goal is, of course, the security of the country. The law went into full effect on January 1, 2009.

It endows the Swedish military monitoring agency, a civilian agency that was confined up until that moment to radio monitoring, to be able to intercept e-mails and telephone communications in and out of the country. Technically, in order to be implemented, this system should apply to all communications in and out of the country.

2) It is in a second move that the *Military Monitoring Agency* distinguishes external communications. This agency is not subject to judiciary or police authorization in order to begin surveillance. No control is exercised on the way interceptions are performed.

The opposition to having adopted this law is not insignificant. The political class is divided on the subject. A protest was organized in front of the Parliament to withdraw the bill, all in vain. A protest site was set up,

7 143 votes in favor, 138 against, one abstention.

without obtaining anything. For the government, the need was urgent because most electronic communications are more and more frequently transmitted through fiber optic cables.

The legal justification is based on *control mechanisms, two commissions that are responsible to conduct the surveillance of interceptions*. According to Anders Eriksson[8], "People have the feeling that this is an invasion of their rights and their freedom. They support the use of such methodology to protect national security, but this law goes too far". The operation of inspection bodies is still being discussed.

C) *Belgium*

The composition and operation of the controlling body with regard to interceptions matters.

1) *Committee R*, a body composed not of parliamentarians, but of experts selected by the Senate, who control intelligence services. A special Senate committee supervises the operation of Committee R.

The latter is formed by three members appointed by the Senate for a term of 5 years. Their mandate can be renewed twice. The president is a judge and the other members are experienced and competent legal experts in matters of policing and intelligence. Only the president exercises full-time activity. At the same time of appointing the three incumbents, the Senate appoints three deputies.

The members of the committee must hold a "top secret" level of security clearance, which means, they are likely to know very confidential information. Their mandate is incompatible with an elective public mandate and with certain jobs or functions "that could jeopardize the independence or dignity of the office". Committee members cannot be part of a police service or an information service.

Committee R is able to act on its own initiative, but, in that case, it is required to provide information to the Senate. It can also act at the request of one of the two assemblies, or at the instigation of either the Minister of Justice or the Minister of National Defense. It also happens to be responsible

8 Former leader of the Swedish secret service and responsible for the regulatory authority with regard to the protection of personal information.

of complaints coming from individuals or to be requisitioned by judiciary authorities.

Committee R works with an investigation service. Appointed by Committee R, the members of the investigation service are usually seconded from a police or intelligence service.

Committee R is therefore an extension of the Parliament while being a regulatory body. Committee R collaborates with the monitoring commission of Committee R. This commission is headed by the President of the Senate, it also comprises four senators appointed after each renewal of the Senate, by ballot, and this is made for the duration of the legislature.

2) *The monitoring commission of Committee R* meet at least once every trimester with the president or with all members of Committee R. It may also meet up at the request of the majority of its members, the president of Committee R or the majority of the members of Committee R. In addition, it is likely to be responsible for any accusation by a member of the committee relating to the infringement by the latter with regard to the law or of its internal rules.

3) *The meetings of the monitoring commission of Committee R are held behind closed doors* and the commissioners are bonded by a confidentiality obligation, even when they are no longer performing their duties.

Committee R is in charge of investigating "the activities and methods of intelligence services, on their internal regulations and guidelines". This means that Committee R, unlike the French *Commission nationale de contrôle des interceptions de sécurité* (National Security interceptions Control Commission) (CNCIS), has no specific expertise in interceptions of electronic communications, but electronic communications interceptions are within the scope of Committee R. This committee may hold as many meetings as it deems necessary, and in order to achieve its objectives, it possesses substantial powers.

It may ask to have forwarded any document that it deems necessary and hear any person whose testimony may be deemed essential. Intelligence service staff members are obliged to communicate to it any "secrets they have received", except those involving court cases in progress. Personnel are

not able to be hidden behind the need to protect some people, since, in these cases, it is the president of Committee R whole rules. The investigation services of the committee can also conduct searches and seizures in places where personal intelligence services exercise their functions. It can collaborate with experts. For their part, intelligence services are required to transmit all of their internal documents to the committee.

Each investigation results in a report that is communicated to the competent minister and the monitoring Senate commission. The minister informed the committee of the measures he or she intends to take in response to the conclusions of the committee. The latter is empowered to question the responsible parties of intelligence services on specific issues. This form of control, which is flexible enough, allows the committee to know how intelligence services address a specific point.

According to the law, Committee R sends an annual report of activities to the monitoring Senate commission. When in charge of an investigation by the House of Representatives or the Senate or when it has been found that the conclusions that had been informed to the Minister had not been followed, or that the measures taken were not adequate, Committee R also prepares a report.

The budget of the intelligence services is included within that of the Ministry of Justice or the Interior and Committee R has no control power, not even financial, *a priori*. On the contrary, during the course of investigations, it can verify the use of funds. In 1995, Committee R had already conducted an analysis of the budgets of two intelligence services; this study was limited to an audit of special funds.

It is the Senate that assigns powers to the monitoring commission of Committee R opposite to Committee R. This committee has, among other missions, the ability to entrust Committee R[9] to conduct investigations and request the reviews of Committee R on legislative and regulatory draft documents. It obtains the information of investigation reports being conducted by Committee R and is able to have any files transmitted to it, including information on ongoing cases.

9 As well as committee P.

Communicating the information cannot be done in case of the endangerment of third parties and there is obstruction to regular and normal functioning of national and foreign intelligence services. In this way, the identity of the parties denouncing will not be transmitted.

The monitoring commission of Committee R sits with the monitoring committee of Committee P to review the annual reports of the two committees before publication. The findings of the two commissions are attached to committee reports. The committees sometimes sit together to analyze the results of an investigation requested by the House of Representatives to Committee R or to discuss the information gathered.

D) *France*

1) *The qualified person and the antiterrorism act of 2006*. The law of January 23, 2006[10] encompasses the fight against terrorism. It concerns, among others, interceptions of electronic communications. In the code of postal and electronic communications, article L.34-1-1 is inserted after article L.34-1. In order to prevent acts of terrorism, individually designated and authorized agents of the police and gendarmerie especially responsible for these tasks may require from operators the communication of data retained and processed by them.

The data that may be subject to this request are limited to technical data relating to the identification of subscription numbers or to the connection to electronic communication services, to the census of all subscription numbers or a connection to a designated person, to the data in relation to the location of terminal equipment used as well as technical data relating to communications of a subscriber with regard to the list of numbers called and calls received, the duration and the date of communications.

Identifiable and specific additional costs possibly incurred by the operators are subject to a financial compensation.

The requests of the agents are motivated by and subject to the decision of a qualified person, appointed by the Minister of the Interior. This person is

10 Law no. 2006-64.

designated for a term of 3 years renewable by the CNCIS based on a proposal by the Minister of the Interior who presents a list of at least three names. Alternate deputies are appointed under the same conditions. The qualified person prepares an annual report of activity addressed to the CNCIS. Duly motivated requests are subject to registration and are reported to the CNCIS. The latter meets regularly with the qualified person. Doubts were expressed about the independence of the qualified person to the extent that he/she is at influence of the Ministry of the Interior.

This notion of "qualified person" is retaken and modified in article 20 of the law of military programming from December 18, 2013. The requests of the agents are always motivated and subject to the decision of a qualified person, but now placed under the Prime Minister. From 2013, the qualified person is designated always by the CNCIS, but at the proposal of the Prime Minister who shall submit a list of three names. Now, the qualified person is located under the Prime Minister solely responsible for interceptions. This guarantee is careful not to forget the needs of intelligence services that are taken into consideration entirely. The qualified person establishes an annual activity report addressed to the CNCIS. If the CNCIS believes that the collection of connection data was authorized in breach of legal grounds, it issues to the Prime Minister a recommendation calling for an end to the collection of connection data[11]. The Prime Minister can obviously ignore this recommendation since he/she is the head of the administration. However, the decision to overrule the analysis of an administrative authority will probably constitute an exception.

The new article L246-2 of the internal security code foresees that the information and documents are requested by the designated agents and duly authorized by the services attached to the ministers in charge of internal security, defense, economy and budget. The ministries of economy and budget were not previously in charge of the application of security interception processes; however, they could already access technical connection data from a ruling of the CNCIS from 2010: the CNCIS considers that the detailed invoices and identifications fall within the preparatory phase to the interception.

11 The recommendation is also brought to the attention of the minister who is responsible for the application.

2) *The Law with regard to intelligence of July 2015*: *the national commission for the control* of surveillance techniques is the body presented within the Law on Intelligence as the one providing guarantees to those people being possibly concerned by interceptions, recordings, "aspirations", in line with a jurisdiction that proves to be the State Council. Is the CNCTR situated in continuity with the CNCIS or does it correspond to a legal segregation?

The first mission of the CNCTR is to monitor the implementation of the legal dispositions; this is *a priori* after numerous talks and the control of the constitutional council.

The CNCTR has a right to access permissions, statements, records, information collected, transcripts and extractions, it is informed at all times, at its request, of the modality of implementation of current authorizations. However, the commission is able to ensure a surveillance of the authorization process. Access is permanent and direct. A crime of obstruction is introduced to the attention of those who would oppose the action of the CNCTR. The latter establishes a yearly public report summarizing its activity.

It can also be seized by individuals. When this takes place, the board proceeds to verify the invoked technique/techniques in order to verify that they have been implemented in compliance with legal provisions. As for individuals, the CNCTR lies in the legacy of the CNCIS. But a collaboration is established with the Council of State, which is a novelty. The law on intelligence establishes a previous mandatory administrative appeal with the CNCTR before any referral is made to the Council of State by an individual.

The nomination of the President of the CNCTR gave rise to a debate in the National Assembly and the Senate. A proposed bill for an organic law filed on May 7, 2015 by Jean-Pierre Raffarin and Philippe Bas provides that the President of the CNCTR must be appointed pursuant to the fifth section of article 13 of the Constitution and that the candidates must be heard by a parliamentary commission within each meeting, the commissions afterward being called to provide their opinion.

The president appoints and chooses the general secretary, officers, judges and contractual agents.

The CNCTR is an independent administrative authority, such as the CNCIS. It consists of nine members, including parliamentarians, judges and a qualified person.

There are four parliamentarians, two delegates and two senators, appointed by their respective assemblies, a "pluralistic" representation of the Parliament is expected (which is in continuation of the CNCIS, since the European Court of Human Rights (ECHR) has demanded representation of the parliamentary opposition within the newly created appellate body, but is explicitly mentioned).

The judges are derived from the State Council and the Court of Cassation, but the designation method varies in the act depending on the jurisdiction. Representatives of the State Council are two judges or former judges of the State Council, who have "at least the rank of state advisor" and are designated by a single person, the Vice President of the State Council. The representatives of the Court of Cassation are judges or former judges "out of hierarchy" of the Court of Cassation.

No grade condition is specified. These judges are appointed, not by one person but by two people, "based on a joint proposal" (therefore, an agreement is essential between the two people responsible for the appointment) of the first president of the Court of Cassation and the attorney general of the Court of Cassation. On the contrary, the general assemblies of the two jurisdictions are not consulted, and the elective designation modality is deliberately ignored. In case of a tie, the chairman has the decisive vote.

The qualified person, who did not exist within the CNCIS and represents the field of electronic communications, is appointed upon the proposal of the chairman of *Autorité de régulation des communications électroniques et des postes* (Regulatory authority for electronic communications and postal) (ARCEP).

The Senate passed amendment number 98, which introduces "a balanced representation among genders". This constitutes an improvement in comparison to the era of the CNCIS, which was largely masculine.

Members are appointed by ordinance. The president of the CNCTR is obligatorily a judge. Therefore, the legal function is carried out by it in

matters of the political function, which was implicitly the case with the CNCIS.

The mandates, with the exception of those from parliamentarians, which encompass a period of 6 years, non-renewable, aim to ensure a certain independence. The end, anticipated or the suspension of the mandate of a member in case of impediment, of incompatibility or serious default can only occur by a decision taken through a qualified majority.

The incompatibility, another traditional guarantee of independence for independent administrative authorities, is stipulated: there is an elective incompatibility for the president, who cannot be the holder of any elected office or other professional activity, there is also financial and economic incompatibility for all members of the CNCTR, who, like the members of ARCEP cannot possess any interest, direct or indirect, "in the services that may be authorized in order to implement the techniques mentioned in article L 34-1 of the Post and Electronic Communications Code (telecommunications, audiovisuals and IT) as well as 1 and 2 of the first of article 6 of law No. 2004-575 of June 21 2004". The law with regard to the confidence in the digital economy has transposed the instruction of June 8, 2000 on electronic commerce. Hence, it is about avoiding conflicts of interest, both economic and political, which is easily understood in view of the purposes foreseen by the law supporting the reform of intelligence.

The budget is attached to the Prime Minister's services.

The CNCTR lies within the relative continuity of the CNCIS but with amplified human and budgetary resources. Its collaboration with the State Council constitutes an additional guarantee. However, this cooperation between the CNCTR and the State Council must confront the legal and political realities of everyday life. The ruling is awaited with great interest.

8.2. European jurisprudence

Indeed, as it turns out, after numerous years the jurisprudence, including that of the Court of Justice of the European Union and that of the ECHR, has played an essential role in maintaining fundamental freedoms: this is true for connection data, for geolocation, video surveillance and the right to oblivion.

II) *This is how the so-called "data retention" directive* [12] *was called into question*. According to article 5, the necessary data to trace and identify the source of communication, the data relating to the identification of the users' communication equipment and the information needed to locate the communications equipment should be stored. The purpose is to ensure the availability of these data "for the goals of research, detection, and prosecution of serious crimes as defined by each Member State according to its national law". Each State defines what a serious crime entails. The instruction was initially a text under the third pillar of the European Union[13], it is only during the negotiation procedure between the Member States that the text has become a draft guideline of the first pillar[14].

A) *This instruction was questioned by some States*.

This questioning was by the countries that have recently joined the European Union, notably Romania and Bulgaria.

In particular, the Romanian Constitutional Court announced on October 8, 2009 that it considers as unconstitutional the transposition of instruction 2006/24/CE. It relies on article 28 of the aforementioned constitution, relating to the confidentiality of correspondence, which is incompatible with the storage of connection data.

This questioning is also by Germany.

In Germany, the conservation of connection data is limited to 6 months. On December 2007, over 20,000 Germans filed a complaint before the German Constitutional Court in Karlsruhe. On December 31, 2007, an appeal was filed by a lawyer on behalf of the working circle with regard to data backup.

B) *The constitutional court of Karlsruhe performed a preliminary decision on March 19, 2008*: the conditions of application limited the consultation of these data by the authorities in cases of serious offenses, such as homicide, tax fraud and corruption. On March 2, 2010, the constitutional court censored the law on data retention. According to the judges, these data were "of utmost importance for effective criminal prosecutions and against the dangers of serious criminality" but they felt that retention "constitutes a particularly

12 No 2006/24/CE from March 14, 2006.
13 Justice and External Affairs.
14 Domestic Market.

serious violation to the secrecy of communicators" because it allows intrusion into the private lives of citizens. The constitutional court emphasized the principle of proportionality and invalidates the transposing act.

The statutory basis for the transposition of instruction 2006/24/EC is under attack in several States of the European Union on a constitutional level.

C) *The development resulted in the jurisprudence of the European Court of Justice on April 8, 2014*[15].

In Ireland[16], Digital Rights introduced on August 11, 2006 an appeal before the high court. It questioned the legality of the legislative and national administrative measures relating to the storage of connection data and demanded the recognition of the annulment of Instruction 2006/24/CE and of Part VII of the Law from 2005 on Criminal Justice[17] allowing the storage of connection data. For the high court, it was not possible to rule on the legal basis of the national legislation before having determined the validity of instruction number 2006/24/CE.

In Austria[18], several appeals were brought before the Verfassungsgerichtshof, seeking the annulment of article 102 bis of the 2003 Act, which would violate the right of natural persons to the protection of their data.

The Verfassungsgerichtshof raised the question of compliance of Instruction No. 2006/24 with the Charter of Fundamental Rights of the European Union. It decided to stay proceedings and ask the question with regard to the validity of instruction No. 2006/24/CE.

Is the instruction 2006/24 in conformity with articles 7, 8 and 11 of the Charter? That is the question being asked.

Data preservation is likely to have an incidence with regard to the freedom of expression guaranteed by article 11 of the Charter. It also falls within article

15 Joined cases C-293/12 and C6594/12 having as their object preliminary ruling requests under article 267 of the TFUE, introduced by the High Court (Ireland) and the Verfassungsgerichtshof (Austria) by rulings of January 27 and November 28, 2012, received at the court on June 11 and December 19, 2012.
16 Case C-293/12.
17 Criminal Justice (Terrorist Offences) Act 2005.
18 Case C-594/12.

7, which protects private life, and article 8 concerning the treatment of personal data. Furthermore, the obligation made in order to retain for a specified duration the connection data[19] violates article 7 of the Charter.

The latter does not violate fundamental rights and corresponds to an objective of general interest.

The acts by the institutions of the European Union should not exceed the limits of what is essential in the achievement of the objectives[20]. The connection data allow national authorities to have a wide range of investigative methods, in particular for the fight against serious crime and terrorism. The directive involves in general people who use electronic communications, including those subject to professional secrecy. To this absence of boundaries is added the lack of objective criteria that would define access to competent national authorities toward this information. The instruction therefore represents an interference in articles 7 and 8 of the Charter. It does not guarantee data destruction at the end of the retention period; it does not state that connection data must be stored in the territory of the European Union. There is no control, required by article 8, section 3, of the Charter, for the respect of the requirements of protection and safety[21].

This is why the legislator of the European Union exceeded the limits of the principle of proportionality. Instruction 2006/24 is declared invalid.

III) *Jurisprudence has also applied since the end of the 20th Century through technical means that can capture images and sounds and through geolocation. This relates to the case law of the ECHR and the European Court of Justice (ECJ).*

A) *The ECHR*

1) *The use of TCV sequences, the "Peck versus the United Kingdom" ruling*[22]

19 Article 5 of the instruction.
20 CJUE, rulings: 2010, Afton Chemical; 2010, Volker und Markus Schecke and Elfert; 2013, Schaible.
21 Aff. C-614/10, Commission vs./Austria.
22 ECHR, Beck vs. the United Kingdom, January 28, 2003, appeal no. 44647/98, section 56.

Facts

In February of 1994, the municipal council of Brentwood approved the use of a closed circuit television system[23]. In August 1995, Mr. Peck, who suffered from depression, attempted suicide by opening the veins of his wrist on a public road; his gestures – of which he is unaware – are filmed by a CCTV camera. The police is notified by the operator and goes to the spot. The officers administer first aid to Mr. Peck, who is saved. Subsequently, a film sequence extracted from the CCTV is disclosed to the media, some images of Mr. Beck in distress are widely disseminated without his consent. On September 14, 1995, the working group of the council with regard to CCTV authorized the distribution of regular newsletters on this device. The first bulletin of the council featured two photographs that show Mr. Peck and accompany an article called "Defused - The partnership between CCTV and the police prevents a potentially dangerous situation[24]". The face of Mr. Peck was not blurred and was recognizable. On October 12, 1995, the newspaper Brentwood Weekly News published a photograph of Mr. Peck, without hiding his face. On October 13, 1995, an article, accompanied by a photograph, appeared in the "Yellow Advertiser". On October 17, 1995, the channel Anglia Television sought and obtained from the CCTV Board excerpts of the video that were programmed and distributed. The face was hidden by request of the CCTV board but this masking was considered insufficient by the of independent television commission. On February 16, 1996, the Yellow Advertiser published an article and a photograph, promoting the benefits of CCTV[25]. The CCTV Council agreed to provide the BBC footage where the image of Mr. Peck appears, which was used in the program "Crime Beat".

Mr. Peck demanded a copy of the broadcasting contract authorization between the CCTV Council and the producers of "Crime Beat". On October 31, 1997, the Council said it could not find a signed copy of the contract. Mr. Peck denounced the publication of the sequence and the photographs and intervened in turn in this regard to the BBC radio and then to the television channels. On April 25, 1996, Mr. Beck filed a complaint against the show "Crime Beat". He recited his right to respect of his private life. This reasoning was welcomed by the BSC. On May 1, 1996, Mr. Beck initiated a

23 CCTV.
24 "Defused-The partnership between TVCF and the police prevents a potentially dangerous situation".
25 Title of the article: "Eyes in the sky triumph".

complaint against the spread of certain images against the channel Anglia Television. The latter proceeds to apologize.

On May 17, 1996, Mr. Peck filed a complaint to the PCC due to the articles published in "Yellow Advertiser". The PCC rejected the complaint: the applicant had acted on the public roads, he could be seen by everyone. On May 23, 1996, Mr. Peck demanded before the High Court the establishment of judicial control of the communication by the Council of images captured by the CCTV: the request is rejected by a single judge.

Through a judgment dated November 25, 1997, the High Court rejected again the requirement of judicial control. Article 163 of the 1994 Law on Criminal Justice and Public Order was not violated. The council was entitled to hand over to the media footage from the CCTV[26]. A request made to the High Court in order to obtain authorization to appeal to the Court of Appeal was dismissed. On February 19, 1998, following a hearing before the full Court of Appeal, Mr. Peck's request to file an appeal's was rejected.

Having exhausted the domestic remedies, Mr. Peck filed an appeal before the ECHR. The appeal was examined.

The law

The United Kingdom argues that the right of Mr. Peck with regard to his personal life is not at stake.

Indeed, according to the United Kingdom, the actions of Mr. Beck took place on public roads; these actions were incorporated into the public sphere.

For the ECHR, the right to privacy supposes an interaction between the individual and others who, even in a public context, fall within the realm of private life.

The monitoring of actions of a person in a public place using an imaging system does not constitute a violation of private life. Mr. Peck does not consider that data collection is in itself an interference of his privacy,

26 "I have some sympathy for the plaintiff, who suffered a violation of his private life.... The board has the power to distribute the footage recorded by the CCTV device... Until English law recognizes a general right to privacy... we must build on the useful guidance contained among other deontology codes", High Court, appeal of November 25, 1997.

according to him, what was an interference was the disclosure to the public of a recording revealing his gestures, in a way that he had not anticipated.

The ECHR mentions the Lupker[27] and Friedl[28] cases concerning the unforeseen use of photographs that had previously been voluntarily submitted.

In the Peck case, the plaintiff was on a public road; however, he was not on this road in order to participate in a public event and he is not a public figure. The sequence was seen to an extent that far exceeded what a passerby would have been able to see for security purposes. The dissemination by the council constitutes a serious violation with regard to the right to respect of privacy. But it had a legal basis[29] and was foreseeable for a person who is surrounded by expert advice.

Was this interference commensurate? The British Government emphasizes the need to protect the lives and the goods of its citizens. It has given the CCTV a key role to avoid hidden surveillance and the disclosed sequence brought favorable publicity for the CCTV. For Mr. Beck, the violation is disproportionate, especially since his face was not hidden. The ECHR argues that the board should have looked for the plaintiff's identity and consent prior to disclosure. Furthermore, the board should have asked the media to mask the images, which would have helped maintaining confidentiality. The ECHR considers that the communication by the Council of images captured by the CCTV was not accompanied by guarantees regarding the compliance of respect to privacy.

2) *The ECHR and geolocation: the appeal of Uzun versus Germany*[30]

Facts

In the spring of 1993, the Ministry of Protection of the Constitution of North-Rhine-Westphalia established a long-term surveillance of Mr. Uzun, suspected of having participated in offenses committed by an anti-imperialist cell. This supervision was carried out initially through visual means, by telephone and mail interceptions. In October 1995, the Attorney General

27 Lupker and other versus The Netherlands, no. 18395/91, decision of the commission of December 7, 1992.
28 Friedl versus Austria, appeal of January 31, 1995, series A, no. 305-B.
29 Article 163 from the law of 1994.
30 ECHR, appeal Uzun versus Germany, September 2, 2010.

from the Federal Court of Justice opened an investigation against Mr. Uzun and an alleged accomplice, S, due to participation in bomb attacks. Surveillance increased, and, in October 1995, the Federal Criminal Police Office installed two transmitters in the car of S, used interchangeably by Uzun and by S. The latter discovered the transmitters, destroyed them, and, knowing that they were being monitored, took measures to escape investigations. For that reason, by order of the Attorney General at the Federal Court of Justice, the Federal Criminal Police Office set up a geolocation device and data were only collected every 2 days. Uzun and S were arrested on February 25, 1996. The Court of Appeal of Düsseldorf dismissed the objection in relation to evidence gathered through Global Positionning System (GPS). The use of GPS is authorized by article 100C section 1.1 (b) of the criminal procedure code. No judiciary decision would have been necessary for GPS monitoring. On September 1, 1999, the Court of Appeal of Düsseldorf condemned Uzun to a sentence of 13 years in prison for attempted murder and bomb attacks. Uzun appealed on points of law, particularly complaining with regard to the use of the trial evidence obtained through surveillance that would be illegal, notably via GPS. The ruling of January 24, 2001 of the Federal Court rejected the cassation appeal as unfounded. Collecting data using GPS was based on article 100 C section 1.1 (b) of the criminal procedure code. According to the Federal Court, due to the serious offenses that were suspected, the use of GPS was a proportionate interference with the exercise by Uzun of his right to respect for privacy. The Federal Court of Justice considered, furthermore, that in the case of resorting to several simultaneous measures of investigations, there was no obligation to provide an additional legal basis and obtain a court decision. It admited that, after the introduction of legislative changes in 2000, article 163 f section 4 of the criminal procedure code stated that any surveillance period greater than 1 month should be ordered by a judge, whether technical instruments are involved or not.

Nevertheless, the need to obtain a court order did not come within the scope of the criminal procedure code or the constitutional law. Mr. Uzun then appealed to the Federal Constitutional Court, arguing that his surveillance from October 1995 to February 1996 constituted a violation of his right to respect his privacy. He argued that article 100 C section 1.1 (B) of the criminal procedure code did not offer a sufficiently precise legal basis for GPS monitoring. According to the Constitutional Court, the expression “special technical means destined toward monitoring” was sufficiently

precise. The harm caused to the plaintiff's rights was proportionate to the gravity of the offenses due to which he was prosecuted.

Having exhausted domestic remedies, Mr. Uzun filed a complaint before the ECHR.

The law

There is no doubt that by proceeding to conduct surveillance through the means of geolocation, the investigating authorities collected, stored and recorded personal data. It is indeed an interference in the private life of the plaintiff, pursuant to article 8[31] of the European Convention for the Protection of Human Rights.

The German Government argues that if there was interference, it was in accordance with section 2 of article 8. This raises issues of accessibility and predictability of the legal basis of the interference. Predictability and compatibility with the rule of law are examined. The Court believes that strict criteria, established and monitored in the specific context of telecommunications, do not apply to cases such as the case in question, relating to the surveillance through GPS of public movements. Domestic law allows prosecuting authorities to order the surveillance of a suspect through GPS, which is performed by the police.

Mr. Uzun argues that the interference was not necessary in a democratic society as defined in article 8 section 2, because the applicable law did not protect him sufficiently against arbitrary interference by state authorities. The ECHR observes that the supervision of a person by placing a GPS receiver in this person's car, associated with other visual surveillance measures of that person, allows authorities, each time that the person uses this car, to follow the movements of this person in public places. We cannot say that the plaintiff was subject to a total and comprehensive surveillance. In addition, the investigation, in which the monitoring was conducted, considered very serious offenses, namely, several attempted murders of politicians through bomb attacks.

The ECHR considers that Uzun's supervision through GPS was proportionate to the legitimate aims pursued and thus "necessary in a democratic society" within the meaning of article 8 section 2. Geolocation,

31 Section 1.

in this context, does not violate individual freedoms and article 8 section 2 of the European Convention for the Protection of Human Rights[32]. The concepts of public order or national security appear implicitly.

In this case law, context has played a decisive role. It is clear that in another case, with less serious offenses, the use of geolocation would not have been considered proportionate to article 8 of the European Convention for the Protection of Human Rights. Uzun's appeal is by no means a permit to resort to the use of geolocation in all circumstances by police authorities.

3) *Video surveillance*

a) *The case of Perry versus the United Kingdom*[33]

Mr. Stephen Perry considers that there was a violation of article 8 of the European Convention for the Protection of Human Rights to the extent that the police filmed without his knowledge for purposes of identification and used the footage as evidence against him during a trial.

Facts

In 1997, several taxi drivers were victims of armed robbery perpetrated by a person pretending to be a client. Being a suspect, Mr. Perry was arrested and agreed to participate in an identification parade on May 15, 1997. He was released in the meantime. Another assault took place and Mr. Perry was arrested again. He did not attend the identification parade. After further attacks and other suspicions, it appeared to the government powers that it was essential to identify the perpetrator of the offenses. Faced with the evasions of Mr. Perry, the police decided to resort to video recording, the authorization to secretly film Mr. Perry for purposes of identification was requested from the deputy director of the police. Mr. Perry was filmed by a continuously running surveillance camera that had been set up to record the whereabouts of the suspects and the police. A technician had adjusted it in order to take clear pictures of the plaintiff. At Mr. Perry's trial, the attorney disputed the evidence obtained through video recording. Is the latter reliable enough to allow the witnesses to recognize the attacker?

Mr. Perry was sentenced to 5 years' imprisonment. The Court of Appeal ruled against Mr. Perry, who appealed before the High Court. The law and

32 ECHR, appeal Uzun versus Germany, September 2, 2010.
33 ECHR, Perry vs. United Kingdom, July 17, 2003.

the internal practice, article 78 section 1 of the law from 1984 on the police and criminal evidence proof, known as PACE[34], and the code of conduct annexed to PACE were examined, without it causing an issue. Mr. Perry was dismissed. Having exhausted all domestic remedies, he filed a complaint before the ECHR.

The law

The first question is to know whether or not Perry was the victim of an interference in his private life. The surveillance of a person in a public place with a photographic device that does not store visual data does not constitute a form of interference of private life[35]. On the contrary, although the voices of suspects in the P.G. and J.H. case[36] had been recorded on a permanent support while they were interrogated by police, this recording was considered to be in violation of the respect for privacy of the persons concerned. The use of video surveillance cameras in places open to the public, if they meet a legitimate goal, does not raise difficulties under section eight. In the Perry case, it is important to know whether the use of the camera and the litigious recordings in question is analyzed as a procedure or a specific personal data use in order to constitute an interference with privacy. Mr. Perry did not expect to be filmed at the police station for identification purposes and, possibly, constitution of evidence. This deception exceeds the limits of the normal or foreseeable use of this type of camera; moreover, the police could have obtained a permit in order to be allowed to use it and the intervention of a technician was essential to achieve the desired setting. The ECHR equates the recording and the use of the video footage to a violation of Mr. Perry's privacy.

Is this violation permitted by the law? Does it have a judicial foundation? The words "permitted by the law" imply that the impugned measure has a foundation in domestic law but also emphasizes the quality of the law. The quality suggests the accessibility and compatibility with the rule of law[37]. The government emphasizes the quality of its internal legislation allowing

34 In the case of R versus Khan (1996), the House of Lords considers that evidence obtained in violation of article eight of the European Convention for the Protection of Human Rights, through the means of a listening device installed in a private home without the knowledge of its occupants, had been declared properly admissible

35 ECHR, Rotaru vs. Romania, no. 28341/95 sections 43-44, Amann versus Switzerland, no. 27798/95 sections 65-67.

36 ECHR, P.G and J.H versus United Kingdom, no. 44787/98§56.

37 ECHR, appeal Kopp vs. Switzerland, March 25, 1998

the performance of video recordings of suspects for identification purposes. The provisions of PACE and the code of conduct constituted a sufficient legal basis for the disputed measure. The debate is not closed either. The trial judge and the judge of the Court of Appeal found that the police had violated all three provisions of the code that should be applied. Indeed, the police officers had not asked Mr. Perry for his consent to have video recorded, they did not inform him of the recording, they did not advise him of the rights at his disposal in this domain: to watch the video, to make any criticisms of its contents and to require the presence of a lawyer during the presentation of the recording before the witnesses.

The ECHR considers that the procedure is not in accordance with domestic law. The British government argues that the production of the video did not affect the fairness of the proceedings. The ECHR considered that the police ignored the necessary guarantees. It recalls its decision of September 26, 2002, which requires to adequately ensure the right to respect of private life. The violation detected is not "permitted by law". Article 8, section 2, of the European Convention for the Protection of Human Rights was not followed.

Video surveillance is, however, a privileged actor of social control. The natural persons involved may notably include employees.

b) *In France*, video surveillance was regulated and amended by LOPPSI 2 of March 14, 2011. Employees are required to be informed of the development of a video surveillance device at their workplace, they should also be informed of the quality of those accessing the recorded images and the modalities of access rights. The principle of good faith to the French social right that excludes any means of evidence that would have been collected without the knowledge of the employee naturally applies to the area of protection[38]. When the company reaches the effective threshold that leads to the creation of a work committee, the latter is "informed and consulted beforehand"[39] and the CE is "informed and consulted before the implementation of the decision in the company with regard to the means or techniques to control employee activities". Indeed, the court of cassation did not accept the means that were not known to the employee: "The employer

38 Court of Cassation, soc.ch., November 20, 1991, 88-43 120 ; Court of cassation, soc.ch., May 22, 1995, 93-44 078 ; Court of cassation, soc.ch., March 14, 2000, 98-42090.
39 Article L 432-2, section one of the code of labor.

cannot implement a monitoring device that has not been brought before the attention of the employee", "The employment of a clandestine surveillance process (...) is excluded".

Surveillance is conditioned by the principle of proportionality. Since 1980, the Ministry of Labor has made known that if the purpose of video surveillance is the monitoring of professional activities, this objective will be considered detrimental to individual liberties by the courts[40], which folded thereafter to this point of view. Video protection is an instrument for the management of human resources. We must strike a balance between power steering, which allows certain surveillance and the respect of freedoms.

In this context, it is important to determine how the obligation of information and the principle of proportionality are applied[41].

When Loppsi 2 was in the process of being developed, the CNIL, authorized to establish penalties since the amendment of August 6, 2004, and the courts, no longer hesitated to comment on the litigation of video surveillance against employees. The main case is in relation to Jean-Marc Philippe institutions, who were faced at the CNIL and the Paris Criminal Court.

Facts

The company Jean-Marc Philippe is a private ready-to-wear company. On December 13, 2007, the CNIL received a complaint from a person who was reporting the absence of a declaration of a video surveillance system and various abuses related to this system. The plaintiff has particularly insisted that the cameras were continuously filming the locations, open or not open to the public, including rooms reserved for staff. The CNIL decided, on February 11, 2008[42] to conduct an audit process on site. On 15 February, 2008, a CNIL delegation went to its headquarters. After 2 hours of investigations, the delegation was forced to interrupt its mission: the general manager of the company was not aware of the monitoring and opposed the permanence of this mission. An ordinance from March 6, 2008, issued by the

40 Min. Resp., JOAN, June 16, 1980, p 2152

41 Read Casaux-Labrunée, *"Henceforth placed at the head of the Labor Code... This principle confirms its vocation to be generally applied to domestic law"*, Employment law, n° 11, November 2008, section 1032 and the following.

42 Ruling n° 2008-023C.

President of the Paris Court of First Instance allowed a delegation of the CNIL to regain its control.

The delegation of the CNIL noted that a video surveillance system, composed of 23 cameras, was located in stores and at the headquarters. Images were recorded continuously on a digital medium. At the headquarters, eleven cameras filmed both public facilities and spaces allocated to staff where goods are not stored. The leaders of the company, the CEO and the General Director, were able to connect to a remote server in order to see images. These latter were also accessible from two supervisory positions. The security measures were hardly operating: the monitoring software was accessible without password; additionally, two servers were freely accessible in so far as there was no locking of the access door and the session. The delegation noted that the video surveillance software was set to save images over 7 days.

Many conclusions emerged. There was no prior declaration with the CNIL. There was no further prefectural appeal authorizing the installation of the video surveillance system. The concerned individuals were not informed: there was indeed a sign referring to the law on January 21, 1995 and the ordinance on October 17, 1996, but this sign was located behind the window of the ground floor of the store in an almost invisible way and no display appeared on the front door of the establishment. In labor contracts concluded after the establishment of the video surveillance system, inserted was the following clause: “the employee is informed that a video surveillance system is installed in the sites of the company”. No additional clause of information was provided for the employment contracts concluded before the establishment of the video surveillance system.

The law

Taking into account the above-mentioned facts, the CNIL proceeded to, by deliberation of May 2008[43], formally request the company to take different measures within 1 month. This is about conducting the completion of the preliminary formalities, to ensure that the purpose of the video surveillance is to fight theft, not to place employees under constant surveillance; the cameras whose presence is not justified by a legitimate objective are removed. It agreed to communicate to the CNIL all measures taken in the company JM Philippe to enforce the right to information

43 Resolution no. 2008-155 of May 29, 2008.

regarding personal data, set up the guarantees required by security and confidentiality treatments that ensure that only authorized persons can access the monitoring software in the computer servers. The formal notice was notified on August 1, 2008 by a registered letter with acknowledgment of receipt.

The company JM Philippe proceeded to perform a declaration of the video surveillance device registered on July 1, 2008.

In a letter on August 29, 2008, the company informed the CNIL that it informed older staff of the presence of video surveillance cameras via email, it also stated that it intended to be able to view the space of the creative workshop that continuously received representatives, converters and delivery of supplies.

The CNIL notifies the company of a report that includes a penalty of at least 15,000 euros. It insists on the fact that the company did not comply with the formal notice of the CNIL from May 29, 2008, with the exception of preliminary formalities.

During the meeting of the restricted formation of the CNIL from April 16, 2009, the company produces written observations and exhibits oral arguments on this file. Several substantial analyses are carried out.

The company did not take any measure to limit video surveillance on the employees. The company argued that the presence of all cameras would be justified by the “handling of merchandise”, by “the free flow of all public and staff”. This means that only the administrative offices “where the employees who have a permanent position are set and who are not intended to be in constant contact with the merchandise” would not be exposed to video surveillance. The CNIL puts forward the principle of proportionality. When a video surveillance device is able to target staff members, names, location, orientation, the operating rhythm of the cameras, the nature of the tasks performed by the persons concerned must be taken into account when the system is installed. According to the screenshots made by the Delegation of the CNIL in an inspection visit, contrary to the claims of the company, offices and permanent workstations are filmed continuously, and employees are under the constant supervision of the employer. This surveillance “appears excessive and the video surveillance device is therefore not strictly limited to the goal of fighting against theft and places the people involved

under a disproportionate monitoring under the objective pursued". This is why the CNIL "concludes that the company has not complied with the formal notice of the CNIL and has not respected the provisions of items 1° and 2° of article 6 of law 78-17 of January 6, 1978".

The controller must inform the people affected by the process, including the purpose, of their right to access, rectify and oppose. On its Resolution No. 2008-155 of 29 May, 2008, the CNIL has formally demanded the company to take all steps in this direction, since the information supplied was considered unsatisfactory. The CNIL states that information provided to company employees is insufficient. Indeed, the objectives pursued, the recipients of the images and the detailed modalities of exercising the right of access, which those concerned are able to know, have not been explained. The formal notice was not followed up on this.

On the contrary, the formal notice was followed up regarding effects in the field of breach of data security requirements: the company has isolated the registration server in a room with a locking system whose access is reserved exclusively to authorized managers. The viewing of images is only available to the legal representative of the company after the use of a password.

The CNIL sets the amount of the financial penalty to € 10,000, meaning € 5,000 lower than the amount proposed by the initial report. This is the case of an exemplary warning, including the lack of proportionality with regard to the surveillance of employees in a continuous manner. This practice is clearly condemned.

The refusal of the General Director of the company to let the CNIL conduct an on-site verification led the independent administrative authority to take hold of the public prosecutor[44] for the crime of obstruction. The Paris Court of First Instance retains the crime of obstruction and rules the sentence of a fine of € 5,000, € 4,000 with suspension.

During this period of preparation of Loppsi 2, the CNIL is therefore ready to protect employees against video surveillance that would be out of proportion with the objective pursued. According to the press release of the CNIL[45], "the deployment of a monitoring device, even if it responds to a

44 Article 40 of the criminal procedure code.
45 22.09.2009.

need for security, should not lead to a generalized and permanent surveillance of the staff, notably in locations where there is no risk of theft".

However, the Court of Cassation does not forget to take into account the legal analysis made by businesses. This appears in particular in the appeal of the Court of Cassation from February 2, 2011, with regard to the lawfulness of evidence by way of video surveillance. A bartender hired on August 1, 1995 by the company Amneville Loisirs was dismissed for serious misconduct. Video surveillance cameras existed and recordings were used as evidence. The case was judged in the Labor Court and then by the Court of Appeal of Metz[46]. A discussion is therefore initiated with regard to the law involving the evidence. The bartender's lawyer reminded the court that employees must be informed of the existence of video cameras and that the recording is admissible as proof only if the evidence collected by the cameras is in accordance with the purpose declared. Yet, the purpose is the safety of the property and the people, and the question arises whether there was no other purpose, such as monitoring the work of employees. By omitting to perform this research, the Court of Appeal would have deprived its decision of its legal basis. Furthermore, to the extent that the employee retains the right to privacy in the workplace, the employer must, if a monitoring is made of those employees that have a relationship of subordination with him, use only means that are not disproportionate in relation to privacy and individual liberties. "By confining itself to assert that the cameras do not violate the privacy of employees while it had itself pointed out that these cameras were working constantly and suggested that the breach of privacy was not just established, but it was especially excessive", the Court of Appeal would have violated article 1121-1 of the labor code. This is not the reasoning followed by the Court of Cassation. The latter argued that the entire staff of the brewery and the bar of the casino was aware of the presence of the video surveillance cameras running continuously, this, in accordance to "regulatory requirements in the matter", consequently, the disputed video recordings constitute a means of lawful evidence.

The implementation of Loppsi 2 marks a turning point with regard to the video surveillance law, now called video protection. The change of name corresponds to an enlargement of the missions. Video protection systems can now be installed to fight drug trafficking and illicit commercial transactions. Now, the CNIL can exercise control to ensure that the video protection

46 Court of Appeal of Metz, soc.ch, January 13, 2010.

system is used in pursuance to the law of January 6, 1978, amended by the act of August 6, 2004. When the CNIL detects a breach of these provisions, it is entitled to issue a formal notice to the responsible party of a device in order to stop. If the operator does not comply with the notice, the CNIL can issue a public warning on his/her behalf. When these measures fail to stop the established infringement, the CNIL can enforce sanctions and request the representative of the State the removal of the video protection device.

The subsequent jurisprudence coming into force with Loppsi 2 is illustrated in particular by the "Oceatech equipement" case.

The company Oceatech Equipement specializes in providing equipment for healthcare professionals, has a staff of fewer than 11 employees and is headquartered in Toulouse.

The CNIL received, on July 27, 2011, a complaint issued by an employee who caught the attention of the supervising authority with regard to the installation of a video surveillance system, which would be located within the company's locations and allow the employer to monitor employees and listen to their conversations.

In pursuance to the decision No. 2011-268c of October 7, 2011, from the president of the CNIL, a delegation of the CNIL performed an inspection visit on October 12, 2011, at the company's headquarters. Seven cameras film places not open to the public, one camera films locations open to the public: this camera, located at the manager's office, has, on its line of vision, a private road that serves the company and other companies, this road has free circulation access throughout the day. The surroundings of the company are also subject to recording by another video device operated by the condominium.

The manager accesses the visualization of live images in real time and the recordings by a terminal server connection type. It happens that the manager has access to a remote connection when he wants to access images from home. The images in real time, unlike the recordings, are with sound. Recordings can be activated manually at all times. Furthermore, the recordings are programmed to be triggered when detecting motion during out of business hours.

The video surveillance device was declared to the CNIL on September 13, 2011, with the objective of securing goods and people. Moreover, in two e-mails sent to employees on July 5, 2011, after recalling the complaints occurred between the two people, a different purpose appeared: "to determine the responsibilities of each person, an audio and video recording system will be up soon". In the declaration on September 13, 2011, the specified period is 1 month. The delegation of the CNIL noted, during the on-site inspection carried out on October 12, 2011, the presence of 4,076 video files, out of which the oldest one was dated July 11, 2011, but the records of automated purges were not contemplated.

The company did not request, as it should have done, an official authorization before the establishment of the cameras.

The information boards relating to the installation of video protection visible during the inspection are located on the front door outside the premises and in the technicians' workshop; they contain no mention of the rights of opposition, access and rectification, which do not appear either on work contracts or in the internal procedures.

There are two incompatible purposes: "the safety of people and of the property" and "the determination of individual responsibilities", which is an actual purpose. This actual purpose corresponds to the number and orientation of the cameras and the possibility of listening to the sound, which were identified during the inspection visit, including the cameras above the employees' workspaces, where there can be viewed, in a permanent manner, the employees' computer screens, the employees themselves, and it is further possible to even hear sounds. This dichotomy between an official purpose, declared effective purpose, is contrary to section 2 of article 6 of the law of January 6, 1978, amended by Law of August 6, 2004, according to which the information is not further processed in a way that is incompatible with the objectives that led to declaration.

According to article 226-21 of the criminal code, "the fact, by any person holder of personal data during registration, of their classification, of transmission or any other form of treatment, to overturn these data of their original purpose, as defined by the legislation, the regulatory act or decision of the CNIL authorizing automated processing, or by prior statements to the implementation of this treatment is punishable by 5 years' imprisonment and

a fine of 300,000 euros". The diversion of goals is common but it can be severely punished.

The installation of video protection puts employees under the constant and continuous monitoring of the employer. Both before and after Loppsi 2, this constitutes a breach to the law of January 6, 1978.

Furthermore, labor law has also ruled on the matter. Article 1121-1 of the labor code states: "Nothing can be brought to human rights and individual and collective liberties restrictions that are not justified by the nature of the task to be performed nor proportionate to the aim pursued". Monitoring of employees is therefore closely supervised.

The signs, the work contracts consulted by the members of the delegation of the CNIL during the inspection visit and the internal rules are not sufficiently informative.

Clients are not informed about the identity of the data controller, the purpose of the treatment of the data, the rights of opposition, access and rectification.

Employees are not informed, not even in their employment contract or in the internal regulations, with regard to the rights of opposition, access and rectification.

Article 32 of the law of January 6, 1978, which is not respected by the company Oceatech Equipement, requires the data controller to provide people from whom personal data information is collected to provide information with regard to the data controller, its purpose, the recipients, rights of access, rectification and, potentially, opposition.

The company did not request prefectural authorization before the formal execution of a video protection installation; therefore, it violates the law from January 21, 1995.

The CNIL served a formal notice to the company Oceatech Equipement within a period of 6 weeks from the notification of the decision to ensure that the installation implementation is exclusively limited to the official purpose of the processing and safety of people and property – and not dedicated to any other purpose – and also to ensure that employees are no longer subjected to constant and continuous monitoring, in line with the

principles of adequacy, pertinence and proportionality of data. The formal notice involves the establishment of an automated purge of records compatible with the duration of 1 month, which appears in the declaration of September 13, 2011, in relative compliance to the aim pursued by the treatment to the rights of opposition, access and rectification, with modification of information boards visible to clients, visitors and employees, with the necessary changes in employment contracts and the internal regulations. Furthermore, the CNIL provides a formal notice to the company in order to request an application for official authorization to be in compliance with regard to the camera facing outside.

Oceatech Equipement took into consideration this formal notice. It modified the device and, in particular, deleted some cameras to meet the officially stated purpose, the protection of people and property. It defined an image storage life that is lawful, proceeds with the individual information of employees. Because the space configuration does not allow filming employees on their workstations, the company is committed to not saving the images, the sounds of cameras during the employees' working hours. The CNIL also notes that these actions were undertaken quickly. Compliance is established; the CNIL decided not to continue to pursue the procedure and announced the closing of the formal notice against the company Oceatech Equipment.

Loppsi 2, through its aspects related to video protection, has entered into the domain of manners. The CNIL rules on increasingly numerous controls and punishments.

Since 2013, it is important to mention the decision of January 3, 2013 from the Union of co-owners "Arcades des Champs Elysées"[47].

The Union of co-owners "Arcades des Champs Elysées" undertakes the management of a mixed-use residential and commercial building on the Champs Elysees. On February 23, 2012, the CNIL received a complaint coming from several security officers whose task is to monitor the union building. These security officers are employees of the company Byblos, an agency specializing in security jobs and work as part of a service provision agreement that was reached with the union. This complaint involved the installation of a video protection system located in the premises of the

47 Resolution of the restricted formation no. 2012-475 of January 3, 2013.

building control station, which could threaten the privacy of the workers in the location by conducting ongoing monitoring of persons employed in security. The trustee reported that the installation of video protection was in order to aim for the security of persons and property and would have been implemented during 2010 following complaints from residents of the building who found an "absenteeism of surveillance officers". This installation proceeded based on a proposal from the service provider in agreement with the trustee.

The device consists of a single camera positioned in order to ensure the visualization of the agent's workstation; it is combined to a recorder that ensures the preservation of images for a duration of 30 days. The images are available to the direction of the monitoring company, the trustee and the head of surveillance team. Furthermore, the whole building is equipped with a video surveillance system of 57 cameras whose control monitors are found in the security station.

On July 19, 2012[48], CNIL provided a notice to the union to remove the camera filming the security post. This formal notice had not been acted upon: the trustee reported that, according to him, the device did not violate the privacy of employees, and that it was necessary and proportionate with respect to the protection of people and goods.

A month later, the president of the CNIL asked the general secretary to undertake a monitoring mission to the Union. During the inspection visit, the following conclusions were dictated: On October 1, 2012, a reporter was designated. After the issuance of the instruction, the reporter notified the Union through a carrier, a document-report listing the violations of the law that seemed to be infringed. After the procedure, the restricted training adopts the decision that analyzes the points of law discussed.

According to the law of January 6, 1978, amended by the law of August 6, 2004, "the responsible party of personal data processing is... the person, public authority, agency or body that determines its purposes and means". Regarding the treatment of the Union of co-owners "Arcades des Champs Elysées", the responsible party is established by several factors. First, the video protection device was installed in the location of a security post. Furthermore, the costs supported by the installation of a video protection

48 Formal notice decision no. 2012-023.

system had been incurred by the trustee who expressed agreement with regard to its installation. Third, despite a change in the service provider company, the camera had not been removed and the new provider did not have physical control of the system. Finally, the trustee informed the CNIL that he was the only responsible of security, he made the statement processing procedure with the CNIL, informed the people involved through posting. It is therefore the trustee who must be considered as the data controller of the Union.

More importantly, the installation of the questioned video protection had to be perceived as disproportionate since treatment placed the security guards present in the building of the security station under permanent surveillance. The question of proportionality arises again before the restricted development. The finding established that the location is equipped with a video protection camera oriented in a way so it can film the employees that are present on the site. According to the trustee's lawyer, the security of the people and the goods justifies the permanent surveillance of the employees of the security post. The Union goes even further: it questions the existence of a right to privacy in the workplace recognized by the Halford appeal[49] within the countries of the Council of Europe. It is based on two facts: employees complained rather late to the presence of the contested camera; in addition, the contract with the first provider was terminated. Consequently, the causes of the complaint would be to look not in terms of the invasion of privacy of the employees but in an internal work conflict at the employing company. Now, new security officers are available and accept the presence of the camera. This acceptance, this agreement, would provide a lawful foundation and legitimacy to the presence of cameras and their recordings.

This reasoning is not followed by the restricted formation of the CNIL. The written and verbal observations of the union show that the treatment in question was intended to ensure not that the security agents were filmed continuously during their presence in the room at their disposal, but the occupants of the building. The safety objective cannot be justified by putting employees under constant surveillance with a mission to provide security unless the need can be demonstrated. Yet, supporting causes of such monitoring cannot find their foundation in the specific risk to which people who are the objects of surveillance are exposed and not in the interest of ensuring the safety of others or their good: the safety of occupants of the

49 ECHR, June 25, 1997.

building is assumed by the network of cameras that are found in the main building and not in the affected location where the security officers are found.

Additionally, the ruling of January 3, 2013 specifies "It is irrelevant whether employees did not complain before the installation of the camera and the new security officers accept the principle as soon as the ongoing nature of surveillance resulting from the treatment in question is not justified by an imperative need of providing security to people and property but out of a will to control the activity of employees". Acceptance by employees therefore does not play any role in the legal or illegal nature of the use of a video protection device. The concept of acceptance was highlighted by the Union. The former subcontractor, the provider of security agents, did not accept the video protection system: they had demonstrated so by filing a complaint. The new security agents accepted its installation; the trustee is satisfied with the subcontractor employee agreement. Without a doubt, it is based on the notion, whether explicit or implicit, of a psychological contract[50]. But the agreement of employees is not taken into account by the controller. The only point that is taken into account is the appropriate and necessary security. In this context, the security objective of goods and people does not apply and the constant monitoring of employees by the vector of video protection has no legal foundation.

The restricted formation limits the amount of the fine to a euro but the penalty becomes public. The advertising is motivated by "the nature of the facts found"[51], which reveals a serious nature. The title of the article by Cynthia Chassigneux[52] is "Financial penalty against the surveillance of employees". "Actualité" is equally explicit: "The CNIL condemns the constant monitoring of employees".

According to Loppsi 2, the Court of Cassation did not have to rule with regard to the legitimacy of video protection, but had to rule on the principle of loyalty and employee information. This is the judgment of January 10, 2012, Mr. X. vs. Société technique française[53].

50 Organizational management.
51 Ruling no. 2012-475 of January 3, 2013 of the CNIL "On the identified deficiencies and the promulgation of the decision".
52 Chassigc.blogspot.fr.
53 Court of Cassation, soc.ch, January 10, 2012, Mr. X versus Société technique française, 10-23.482.

Facts

Mr. X and other employees of the cleaning company Technique française du nettoyage had been affected by a corporate client, Guillet. They took hold of the labor court to obtain the payment, including clothing premiums. Their employer requested and obtained on September 3, 2008, an ordinance on request that indicated a bailiff to view the video surveillance camera recordings at the entrance of the company Guillet during the period of April to August 2008: the aim was to establish a record of the hours of arrival and departure of employees in order to achieve a comparison with actual business data prepared by the team leader. The minutes drawn up on September 18, 2008 were produced by the employer under the employment of a tribunal procedure. Employees and the Union of CFDT services of Maine-et-Loire requested an interim withdrawal on appeal and the nullity of acts.

The law

In order to dismiss the employees and the Union of their claims, the ruling of the Court of Appeal holds that the strengthening of the video surveillance by the company Guillet did not aim to conduct a surveillance of employees and proceed to inspection for labor provider companies and only monitor local access doors to enhance security; the employer proceeded to notify, on 20 May 2008, its employees of the existence of this device, it has therefore fulfilled its duty of loyalty by information to which it was not for that matter obliged[54], since the process had been set up by the company's client; in this context, the records would have been lawful means of evidence.

The Court of Cassation pointed out that if the employer has the right to monitor the activities of employees during working hours, it is not entitled to authorize the records as evidence of the video surveillance system placed on the site of the client company, allowing employee monitoring, which have not been informed beforehand of the existence of the device. This disclosure requirement is mandatory. The letter of May 20, 2008 did not explain to the interested employees that they were being filmed, which allowed checking their times of arrival and departure. For these reasons, the social chamber breaks the judgment of the Court of Appeal.

Furthermore, the social chamber reasons that the law concerning the confirmation of the interim order made by the District Court of Saumur, who

54 Article L122-4 of the labor code.

dismissed the request of Mr. X and eight other people asking for the withdrawal of the ordinance of request made on September 3, 2008, by the President of that jurisdiction and the annulment of the subsequent acts. According to the Court of Appeal, it was no later than April 28, 2006, that the work council of the company Guillet was notified of the installation of cameras "at each entrance". These cameras are installed at each staff entrance in the company only to monitor intrusions and are not capable of checking times.[55] In addition, since May 20, 2008 the company Technique française du nettoyage warned all its employees working on "the Guillet site", by mail, of the video surveillance system installation and setup. There is no need to ask the Court of Justice of the European Union for a preliminary ruling that would be irrelevant, says the Court of Appeal.

According to the provisions of the labor code,[56] video recordings are strictly prohibited when carried out without the knowledge of the employees, without having the employee representative committee informing of the establishment of such a system. The Court of Cassation[57] stipulated that the employer was not required to disclose the existence of processes installed by the company's clients, which involved its own employees, including, as in the case of the companies TFN and Guillet, the implementation of cameras agreed by the company Guillet aimed to control the access doors of its locations to strengthen security after repeated thefts. Mr. X and the other plaintiffs reported a complicity between the two companies but this complicity, which would aim to conduct surveillance of employees, is not obvious because the company Guillet did not have subordination powers over the employees of the company TFN and would not have invested in order to monitor the employees of its service provider. The Court of Appeal proceeded to also argue that since May 2008, employees of the company TFN had been warned of the an increased video surveillance of the client company[58].

The surplus vigilance of the company Guillet marked by the installation of new cameras is not intended to monitor the employees of the company

55 Which is controlled by other methods.
56 Article L122-4 and L2323-32.
57 Social chamber, April 19, 2005.
58 "The company TFN was fulfilling its duty of loyalty opposite its employees by this preliminary information to which it was not obliged", quoted in the court of cassation, social chamber, January 10, 2012, Société Technique française.

TFN, but rather to exclusively exercise control over local access doors. Accordingly, for the Court of Appeal, videotapes constituted a lawful means of proof, since according to social law, lawful evidence means is a piece of evidence that is not obtained without the knowledge of employees.

This reasoning does not convince the Court of Cassation: on the basis of the principle of loyalty and article L1222-4 of the labor code, the employer is not entitled to use a video surveillance system that allowed monitoring and controlling the activities of employees without having the latter previously informed. Yet, the Court of Cassation proclaims the following: "such a principle is applicable regardless of the workplace and the responsible party of the video surveillance", it is of little importance the concept of service provider or client company. The Court of Cassation takes the legal opposite of the Court of Appeal: "retaining that it constituted a lawful mode of evidence, a video recording made by a device installed by the client company when it had not intended to monitor the work of employees of the service provider, but only monitoring the access doors to the premises while monitoring access gates to control the entrance and exit work hours, and, therefore, the activity of employees", the Court of Appeal violated the principle of loyalty.

Finally, the Court of Appeal seems to have forgotten the concept of good faith. Indeed, the mail sent to all employees, with regard to the new monitoring system installed by the company, would have, on the basis of a simple deduction, informed all employees of the service provider company that video surveillance had increased. This is not consistent with reality. The mail mentioned by the Court of Appeal deals only with the establishment of a monitoring system for the opening of emergency doors. This e-mail was intended solely to instruct employees to "imperatively enter and exit through the main entrance". The Court of Appeal has "distorted the mail" and violated the Civil Code[59]. The information of the employees did not exist and the registration system had no legal foundation.

After Loppsi 2, the CNIL and the Court of Cassation appear in relative agreement regarding the employees, whether it is about information or proportionality. Nevertheless, it is the CNIL, as part of its supervisory jurisdiction, which is the main vector and engine of the jurisprudential construction in this domain.

59 Article 1114.

In many situations, the employees "accept" to a greater or lesser degree, through the adherence of a management system, or, more often, by habit of the intrusion of information technology, which builds a tacit ideology of proactivity in a body of diverse controls, the video protection devices. However, the process is not general or widespread. Some employees experience as an unbearable infringement on their privacy the permanent and constant presence of cameras and refer to the CNIL. Before this dichotomy, the doctrine is shared. Human rights defenders wish that the use of cameras to monitor employees is reduced and is justified by legal purposes. Other doctrinarians, more sensitive to economic freedoms, the rights of the company and the employer, consider that it is important to overcome this antagonism. They are located in the line of Charles Hannoun [HAN 08]: "The financialization associated with the liquidity of the company, that of labor. It reduces the company a detached numerical representation of concrete realities, whether it is the production tools transferable to infinity... or employees treated as a freely adjustable user value, regardless of the constraints of its management and other dimensions of the work collectivity". Could we reach a balance that satisfies the advocates of human rights, the advocates of human resources management, and the management controllers? The question remains open.

4) *Personal data, with big data, open data, the cloud, play an even more significant role in the tense relationship between the economy and the protection of individual freedoms. This is particularly the case for the right to oblivion*.

In the matter, it is important to address an important ruling of the Court of Justice of the European Union, Google vs. Spain[60].

On March 12, 2014, the European Parliament passed at first reading a draft regulation. On the same day, the European Parliament also passed on first reading a draft directive to enforce the rules and general principles relating to data protection in police and judicial cooperation in criminal matters. This text introduces guarantees that are strong enough for the personal data of the citizens of States of the European Union transferred to countries not belonging to the European Union. These texts provide

60 CJUE, May 13, 2004, Google vs. Spain.

information on the right to the deletion of data provided by Instruction 95/46, and establish a right to oblivion, increasing the fines imposed on corporate offenders, up to € 100 million or 5% of their estimated total turnover.

It is under the right to digital oblivion that the ECJ carries the case law in the judgment of May 13, 2014 of Google versus Spain[61].

Facts

The case started in 2010 with the complaint of a Spanish citizen, Mario Costeja Gonzales, initially with Google Spain and Google Inc., unsuccessful complaint, then with the Spanish Agency of data protection[62], which ruled in first degree on applications regarding the protection of personal data. The complaint involved La Vanguardia Ediciones SL, the publishing company of a Spanish newspaper, Google Spain and Google Inc. Mr. Gonzales noted, in support of his complaint, that when someone, an Internet surfer, entered his name into the Google search engine, the list of mentioned links to two pages of the newspaper La Vanguardia, dated January and March 1998, showed a sale of a building that had been seized in non-payment of social security debts. According to Mr. Gonzalez, these references were no longer adequate: the debts had been cleared for a long time, that is why Mr. Gonzales requested to La Vanguardia to be ordered to remove or edit the pages in question so that his personal data would no longer appear. He also requested to have Google Spain or Google Inc. to be ordered to remove or hide the personal data implicating him in this issue.

The data protection agency rejected the complaint brought against La Vanguardia: it considered that the information was legally published in the newspaper, to the extent that it was a notice of a judiciary sale, a legal ad. On the contrary, it asked Google to adopt the necessary measures to withdraw the data from its index. Google Spain and Google Inc. referred to Audencia Nacional[63] in order to obtain the reversal of the decision of the AEPD.

61 CJUE, Grand Board, May 13, 2014, aff. C-131/12 google Spain SL and Google Inc/agencia Española de Protección de Datos and Gonzales
62 Agencia Española de Protección de Datos, AEPD
63 Appellate Court.

Before Audiencia Nacional, the debate regarding the responsibility of the search engine and the question of the responsibility of the editor of the source site is not contemplated.

The law

The Court of Justice of the European Union (CJUE) rules on a preliminary reference from Audencia National for interpretation of Instruction 95/46. The CJUE rules that the activity of a search engine should be classified as "processing of personal data"[64] and that the operator of the search engine should be treated as a "responsible party of personal data processing", in the sense of Instruction 95/46.

For the CJUE, the provisions of the instruction of October 1995 are applicable to the activity of indexing personal data carried out by a search engine and the operator must ensure that its activities comply with the requirements of the instruction.

Another question of the ARPD concerns the territorial scope of the instruction: the CJUE considers that the instruction applies where a parent company, which performs the processing of personal data outside the European Union, has a subsidiary located in a Member State of the European Union whose business is the sale and promotion of advertising space, as is the case of the company Google. This issue is justified because, within the company Google, the parent company Google Inc., it exerts only a business geared toward an advertising network.

The CJUE then considered the extent of the liability of the operator of the search engine in the event of indexation of personal data and therefore found a right for digital oblivion, an offshoot of the right to respect of privacy[65]. The implementation of articles 7 and 8 of the European Charter of Fundamental Rights led to the removal, under certain conditions, of hyperlinks of a search engine linking to websites where personal data were included.

64 Article 2 (b), instruction 95/46.
65 The CJEU expressed its decision by an explicit reference to articles 7 (respect for privacy) and 8 (protection of personal data) of the Charter of Fundamental Rights of the European Union.

What are the conditions of implementation of the right to oblivion established by the CJUE in this ruling? In which cases is it possible to achieve the deletion of hyperlinks from a search engine?

According to the CJUE, the operator of a search engine is required to remove from the list of results found by typing the name of a person, the links that point to websites containing personal data relating to that person, if the processing of personal data in question is incompatible with instruction 95/46. The incompatibility can "result not only of the fact that these data are inaccurate, but, in particular, also from the fact that they are inadequate, irrelevant or excessive for the purposes of the processing, that they are no longer updated or are stored for a duration longer than necessary, unless their retention is necessary for historical, statistical or scientific objectives"[66]. Under these conditions, if the disputed personal data fall into one of these categories so that the individual is entitled to have the links from the search engine deleted, the existence of damage resulting from "the intrusion with regard to the information in question in the list of results" does not have to be demonstrated[67].

These criteria of implementation of the right to oblivion imply some questions (What is understood by "necessary duration"? What is understood by "irrelevant or excessive data"?) and is broad in scope. Therefore, there is a risk of mass deletion of hypertext links from search engines.

The CJUE is interested in both data processing initially contrary to Instruction 95/46 and the processing of data that becomes contrary to Instruction 95/46 with the passing of time[68]. The Court notes in this regard: "Even a lawful processing of accurate information can become, over time, incompatible with the instruction when this information is no longer needed in view of the goals for which it was collected or processed. This is notably the case when they appear to be inadequate, or they are no longer pertinent or are excessive with regard to their purposes and of the time that has passed"[69].

The right of digital oblivion is the "possibility offered to everyone to control their digital traces and their private life as well as their public-online

66 Section 92 of the judgment of May 13, 2014
67 Section 96 of the judgment of May 13, 2014.
68 "Exceeding duration as necessary".
69 Section 93 of the judgment of May 13, 2014.

life"[70]. The CJUE believes that the interested party is able to obtain the same erasure when the information is not deleted from websites where he/she appears and, as the case might be, even when the publishing on these pages is lawful. It is therefore not necessary to address the publisher of the source website before requesting deletion from the search engine. It is possible that some data that are not found on Google anymore could be found through another search engine, which could cause users to turn away from the latter if the deletion requests grow and multiply, and since the other search engines will not have the same obligation to deindexation as Google. This decision goes against the general counsel, who believed in June 2013 that Google was not responsible for personal data appearing on its pages.

Nonetheless, this right is not absolute. While recognizing the right of users to digital oblivion, the CJUE recalled that the deletion of links from the list of results clashes with right to public information. A fair balance will be looked for between this right to information and the right to oblivion. The CJUE mentions, nevertheless, that erasure is the rule and maintenance is an exception ("The rights of the person concerned (...) prevail (...) as a general rule", *the balance depends "*in particular cases (...) of the public interest towards having this information, which may vary, particularly depending on the role played by that person in public life"[71]).

The notion of "public person"[72] is well known as an exception with regard to privacy, the courts and supervisory authorities should understand the adverb "particularly" and proceed to define the outline of the exception.

According to the CJUE, the erasure requests should be transmitted directly to the operator of the search engine, in case of no answer or refusal, the person may appeal to the regulatory authority or the judicial court. It is for the operator, Google, in this case, to determine before any claim, if an application is legitimate or not.

This ruling, like all the decisions taken by the CJUE, benefits all citizens of the European Union, regardless of nationality, but only citizens of the European Union. It is imposed toward all the national authorities and courts of the Member States, which would be subject to a referral of a similar

70 Activity report of the CNIL 2013, p. 16.
71 Section 81 of the judgment of May 13, 2014.
72 The summoning of the right to oblivion is excluded when it entails a public person and the interference with their fundamental rights is justified by public interest.

problem. The obligation of deindexation, which currently applies to Google, will be extended to all the search engines.

Google has posted online "right to oblivion" the form in order to gather requests for link deletions. This form is widely used.

The right to oblivion for minors has become a subject of study in many Western States. In California, the right to oblivion for minors came into force on January 1, 2015. In the United Kingdom, IRights started a campaign in 2015 regarding the right to oblivion for minors, focusing on the slide caused by adults due to data, photo content, particularly in social networks at the time of their underage.

In France, the digital act embodies the right to oblivion for minors. It is about the ultimate accolade of a request sourced from the civil society and also from some deputies.

The European decision seems rather favorable to human rights, but the concept of "fair balance" does not allow us to forget that this ruling meets the principle of business freedom, freedom of movement of goods and services already inducted in the Treaty of Rome.

Furthermore, the proposed European regulation emphasizes the prior consent of the concerned people, the right to oblivion. Even if compromises have emerged, surveillance through various digital technologies and the technologies that accompany digital technology tends to develop, first and foremost in Western countries, which control most of the informational richness, and also in emerging countries, and sometimes in developing countries.

This applies particularly to communication technologies, but also genetic files. The actors are always the States, among which the agreements have been passed, and also large companies and non-governmental organizations.

8.3. The monitoring continues to develop in the communications sector

This is true for the United States, the United Kingdom and France.

I) *In the United States, in 2015, the Patriot Act and the FISA law led to examinations that generated heated discussions*

A) *The Freedom Act*

Before June 1, 2015, the vote for the extension of certain articles of the Patriot Act was scheduled, which allowed security services to obtain computer data held by commercial companies and individuals without authorization from a judge and without obligation of information. The FISA law merely implies for claims to be filed before a FISA court[73] within the framework of "an investigation against international terrorism": according to section 215 of the "Patriot Act", a warrant is requested from a FISA court to get the operators to provide all the metadata of their customers residing in the United States or of American citizenship. Yet, a court ruled that Section 215 was not a sufficient legal foundation to justify the request: second, a federal court ruled on May 7, 2015 that the metadata surveillance program implemented by the National Security Agency (NSA) was not justified within a legal framework: the court noted that section 215 of the Patriot Act was wrongly used by the NSA and the American government to implement this program. The case law was ruled in that sense, only a law is able to "correct" the inflections of the court. Admittedly, the justice had not ordered the end of the surveillance due to a simple reason: section 215 was set to expire by the end of May, 2015. A bill that modifies the way telephone metadata is collected from Americans was passed with mixed support (democrats/republicans) by the Judiciary Committee of the House of Representatives, an adjacent text was proposed to the Senate, but in the Senate, certain Republicans defended the renewal of section 215 as it existed earlier, before the decision of the federal court. On May 13, 2015, the House of Representatives approved the text intended to replace section 215 of the "Patriot Act", these provisions would allow revising certain methods, which the NSA uses to collect communications data, while continuing to perform surveillance on American citizens. On May 31, 2015, the Senate did not get to rule on the text. So, since June 1, 2015, at midnight and for a few days, a part of the Patriot Act, through which the NSA collected communications data from American citizens[74] could not be officially applied anymore. Any

73 Unknown to the public.
74 Time of calls or messages sent, frequency, time spent on the phone.

"antiterrorist" investigation launched since June 1 forward, and while waiting for a new vote from the Senate, was not supposed to authorize the collection of connection data. The Presidency has increased the declarations of condemnation with regard to the responsible parties for this situation. The temporary suspension of these surveillance techniques allocated to the NSA was presented as catastrophic and mention was made of "national security" in order to condemn the unpatriotic attitude of the senators. "When it comes to dealing with such critical issues as the national security of the country, senators must, individually, put aside their partisan motivations. The American people deserve nothing less" said government spokesman Josh Earnest. This new legislation is referred to by the press as the "Freedom Act".

On June 2, 2015, the Senate passed the "USA Freedom Act", which limits certain powers that appeared in section 215 of the "Patriot Act", but in counterbalance of an extension of certain articles of the former section 215 of the "Patriot Act", relating to the devices used by the NSA to monitor American citizens.

Authorities still have the possibility to be informed of metadata in real time, according to specific criteria[75], related to terrorism. This applies to natural persons, accounts and single terminals. In order to obtain this information, authorities must justify a "reasonable and detailed" connection with terrorism, but this requirement of a reasonable connection does not apply in case of emergency, yet, it is often resorted to in case of emergency. The law also foresees a reform of the FISA court[76]: the FISA court can, in particular, seek out five external individuals for help, if there are needs involved that justify such a measure, in particular in order to decide on new interpretations of the law. And the defense is by no means depicted in this court of justice. It is up to the director of intelligence to decide on the eventual declassification of a decision that would imply a new interpretation of the law[77].

The text refers to telephone metadata. It encompasses a small component, as gathering targeted information is the collection of information that takes

75 "Specific selection term".
76 FISA Court.
77 See: "the specific criteria".

place in the United States. Nothing has changed in relation to the surveillance performed by the NSA abroad.

In fact, the powers guaranteed to the NSA by the new law are very significant and very broad and it is not obvious that it is located in the lines with the case law of May 7, 2015.

The representatives and senators who voted for this law did so for very different reasons. Some, notably the democrats, were acting by orderliness: the White House wanted the "USA Freedom Act" to be voted in; disciplined, these representatives and senators followed the wishes of the Presidency. Among the Republicans, who disapproved of the law of May 7, 2015, the law was designed to follow a jurisprudence: they are opposed to this approach and have sometimes voted against the law. Other Republicans see the "Freedom Act" as an acceptable compromise that allows us to abide the decision of an American court, while maintaining nearly all the powers granted to intelligence services, notably the NSA, so they gave their votes.

In the majority of cases, the voters are not "liberal" in the American sense of the term, but instead give priority to the conversation of national security, to the protection of devices set up by public authorities to fight against terrorism and protect the fundamental values of American patriotism. The "Freedom Act" is situated in continuity of the "Patriot Act": let us remember that the "Patriot Act" was foreseen for a relatively short duration, with the choice to limit individual liberties of American citizens within a time limit that did not have a determinate character. Yet, the law of June 2015 makes it possible to extend largely not only section 215 of the Patriot Act, but also the surveillance measures initiated by intelligence services, beginning with the NSA.

When the "Patriot Act" was passed, just one member of Congress abstained, this unanimity translated the attachment to national and nationalist ideals that are the prerogative of the United States, the first military power in the world, with regard to being able to intervene and impose all surveillance measures anywhere it appears appropriate to its interests.

B) *In October 2001, the defense organisms of human rights* had remained dormant, even though the main rights of American citizens were under

quota. These NGOs probably did not want to depart from the overall momentum that had gathered the Americans against internal and outside enemies. But after a few years, these NGOs initiated actions, filed complaints in court that sometimes succeeded: they readopted their original purpose, the defense of the American Constitution and the human rights linked to Western democracy.

The ACLU and the EFF[78] demonstrate their opposition to the Freedom Act. They consider the law to be inadequate with regard to individual and collective freedoms. The collective "Fight for the Future" had expressed their desire, as noted in Slate.fr, that the law was "considerably improved or abandoned", being very aware that the collection of connection data by the NSA would resume quickly and under similar conditions to the original "Patriot Act".

Some Western observers have perceived in the "Freedom Act" a renewal of American democracy, manifested in lively debates in Congress as well as in the observations of human rights organizations. These remarks were inserted within national contexts where surveillance was institutionalized and where opposition to this institutionalized surveillance was timid, not to say inexistent.

But within the United States itself, mass surveillance has been consistently confirmed under Obama presidency and it is unlikely to be challenged after the next American elections: between 2001 and 2015/2016, a system was established with connection data and metadata that are the subject of a systematic collection through the new law. Data are not gathered in an automatic manner; however, in each case, with direct requests from private telecommunication operators. The system will perhaps take – it remains to be seen – a little longer to come into action, but the process is identical in nature and intrusive. The American example is the main reference for metadata collection and therefore it is significant that "the evolution" of 2015 was reserved. The implemented systems in most Western democracies are inspired to a lesser or a greater degree by what happens in the United States and that is why the approach of the "Freedom Act" was necessary and leads to rather pessimistic conclusions about the possibility of getting out of the Patriot Act "model".

78 Electronic Frontier Foundation.

The American example of the U.S.' Freedom Act is not isolated. The main allies of the United States within the NATO seem to want to imitate, at least in part, American references.

II) *This is notably the case of Canada*. Following the media coverage of the attacks (this media-political process[79] is pretty much used everywhere, whether it is France, the UK, the United States, etc.), two Islamist attacks in the Fall of 2014, where two soldiers – representatives of the Provinces and the Federal state – lost their lives in Quebec and Ottawa Parliament, a law on intelligence was passed on May 6, 2015.

This law, C-51, provides to public authorities a legal arsenal in order to limit or even prevent Islamist youth departures toward combat zones. For a long time, the role of the Canadian Security Intelligence Service[80] was to gather information in order to participate in the defense of national security. Now, the CISC is organized to prevent suspected criminal activities of potential terrorists: the Internet accounts of the alleged criminals will be able to be hacked and interceptions will be possible for Canadians and their families suspected of nurturing criminal intentions.

With the goal of facilitating the arrests of suspected terrorists, federal agencies will be able to address a judge during hearings that will have a secret nature and where no defense lawyer will be present. In addition, the transmission over the Internet of "terrorist propaganda", the sharing of data through the Internet in order to prepare illegal actions will be considered a "criminal" act, regardless of the intention of the user in question.

This law was initiated by the conservatives and approved by most of the opposition. It was passed by the Lower House of the Parliament of Canada by 183 members of the Parliament against 96 and some amendments proposed by a fraction of the non-democrat opposition were rejected.

The opposition to the law has quickly manifested. Before the adoption of the provisions, the newspaper "The Globe and Mail" although it had supported the conservatives in the 2011 elections challenged the legal certainty of the text. An editorial titled "C-51: An Act passed soon and still

79 That some connect to the "strategy of suspicion".
80 SCRC.

very obscure" drew attention toward the lack of clarity on a number of items. The newspaper also highlighted the fundamental rights and freedoms, to which Canadian institutions have seem attached for so long. "The drastic measures of the law constitute an unjustified infringement of the rights of Canadians". Many other media organizations joined forces to defend those rights that seemed threatened by the C-51.

This campaign is endorsed by officials, including the Privacy Commissioner, who has the task of protecting personal data, and who considers that the C-51 violates the fundamental rights of Canadians. This point of view is shared by the majority of legal associations who have been concerned and have drawn parallels between law C-51 and the Universal Declaration of Human Rights, the International Covenant of Civil Rights and the texts which at a Province and Federal State level proclaim the fundamental rights of Canadians.

The civil society also partly mobilized. This is particularly the case of Native Canadian Americans, who, for the most part, maintain a difficult relationship with intelligence services, to the extent that many Canadian Amerindians, in an associative framework, militate against certain development projects of natural resources. These Native Canadian Americans associations informed that they intended to mobilize "vigorously" against law C-51, which is perceived as undemocratic.

A petition signed by 200,000 Canadians contended that this reform will transform intelligence services into a "secret police", which violates the Constitution and establishes a "mass surveillance".

Even if the Supreme Court does not accept all the provisions, the new Canadian Law on Intelligence is included within the Western current mentioned above.

III) *In the United Kingdom*, a law is expected to strengthen the powers of surveillance and intelligence. This law was announced during the speech by Queen Elizabeth II on May 27, 2015. A previous and controversial bill[81] was not able to obtain a majority, due to the opposition of the Liberal

81 It had been dubbed by the mainstream press the "snooper's charter".

Democrats. The defeat of The Liberal Democrats during the British general election of 2015 paved the way for the passing of the legislation going in the same direction as that which had been postponed, but with a certain number of revisions.

British intelligence services have experience of Internet piracy. The Government Communications Headquarters[82], associated with the NSA, infiltrated several gaming platforms online, including World of Warcraft, Second Life and Xbox Live. In February 2015, a reliable document revealed that the British and American agencies had entered computer networks of the first SIM card manufacturers in the world, Gemalto. GCHQ were also involved in the reverse engineering of antivirus software.

The law obliges Internet service providers to conserve all their customers' connection data. Internet services, community networks, e-mail providers or storage space provide access to unencrypted user data within the framework of an investigation. Big technology companies like Facebook, Apple, Google and WhatsApp will need to allow access to public authorities.

A partnership has been signed between the Government of the United Kingdom and five private companies that have the task of analyzing the communications performed by British Internet users. The law is the "Communication Data Bill", which was defended by the Home Secretary, Theresa May. The goal is to detect "suspicious" behaviors in order to fight against terrorism and facilitate the intervention of security forces at a specific location. With the "Communication Data Bill", Internet service providers are required to keep exchanges for 12 months.

The text also grants the electronic communications regulator, Ofcom, with new powers of censorship, which would allow blocking television channels with "extremist" programs. The Home Office will be able to prohibit and disband groups which are considered to be resorting to violence or advocating violence.

This law obviously holds a special interest with regard to terrorism, and also in the surveillance of communications "of pedophiles and other large criminal organizations". This is actually to reconnect with the "snooper's charter".

82 GCHQ.

In the United Kingdom, specialized NGOs in the defense of human rights have violently critiqued the bill of February 2015 and issue the most extreme reservations about the current legislation to the extent that it is inconsistent with collective and individual freedoms guaranteed in a democratic state.

IV) *In France, the Law on Intelligence has been validated almost entirely by the Constitutional Council*. The only noticeable change – except for international communications – encompasses the obligation to resort to the Prime Minister's approval and the opinion of the CNCTR, even in cases of an operational emergency.

The provisions considered as the most liberticidal ones were maintained, in spite of the outcry of associations defending human rights, or the critiques of "La Quadrature du Net". The IMSI Catcher, the algorithm, all participated in a mass surveillance company that is justified by the antiterrorist threat while reports of Jean-Jacques Urvoas in favor of a better Intelligence Policy could be consulted in the Parliament since 2013 and 2014. The objectives were considered consistent with the Constitution, including collective violence liable to undermine public peace. However, this new ground had been the subject of lively debate by some Members of the Parliament and senators. What does the legislator perceive as "collective violence"? Is it understood as assault, which are the offenses that fall under the criminal code? Can this term designate authorized manifestation that could be degenerated? How can we measure and quantify the "serious breach of public peace"?[83] These remarks are not taken into account by the law commissions and the parliamentary majority[84], the latter just rely on public

83 Sergio Corodano, green member: "I think that we can in a non-violent, pacifist manner, challenge the republican forms of the organization of our country. This seems to be the case of some anarchist movements, of some monarchist movements, elsewhere, who do not do so by violating the law. That seems to me the case as well of some regionalist movements that challenge the republican form, and its supreme outcome, which is the Jacobin Republic as we know it. The drafting of the Law Commission implies that we could monitor nonviolent political movements, which exceeds the monitoring of dissolved movements..."? National Assembly, second session of April 13, 2015.

84 It is not the case of the green representative Aurélie Filipetti, who argues: "The field seems too broad in relation to violations of individual freedoms and privacy, which are carried by these intelligence techniques… The term "collective violence likely to undermine national security seems to me too broad and imprecise", National Assembly, second session of April 13, 2015.

authorities[85] to bear a fair assessment and on the "collective violence" and "the serious violation of public peace". The constitutional council only marginally censors all the articles.

In 2016, a new antiterrorist law[86] authorizes the IMSI Catchers in the judiciary field (delinquency cases and organized crime), on the capture of images and sounds in private spaces[87] or buildings for residential use, an authorization is now possible on the phase of flagrancy investigations and preliminary investigations, ruled by the judge of freedoms and detention. The prosecution is therefore present at this level of the procedure, upstream.

In the United Kingdom, a law with regard to surveillance also gave rise to debates in 2015 and 2016. In November 2015, the bill intended to extend the powers of the police and surveillance agencies, notably the interception sector, was presented by the British Home Secretary, Theresa May. After their electoral victory in May 2015, the Conservatives were mostly interested, as they were in France, with regard to the metadata of British citizens: intelligence services are able to visit the sites on the Internet and providers are required to keep the exchanges for a year. To access these data, surveillance agencies – such is the proposed "guarantee" – must obtain a warrant from a judge.

V) *In fact, these texts are part of a broad partnership selectively commissioned by the NSA*, that began in the 1980s. An article from 1989 was recently declassified from the internal review of the NSA[88] and emphasizes the interest by the American agency to develop a collaboration with the countries "Third Party Nations". Initially, the cooperation was limited toward English-speaking states, Australia, Canada and the United Kingdom, but it expanded. All NSA partners have access to innovative surveillance technologies and NSA partners facilitate access to interceptions. Intelligence

85 The Minister Bernard Cazeneuve says: "Some forms of violent radicalism threaten the foundations of the Republic and its values: we must take preventive measures in front of them", National Assembly, second session of April 13, 2015.
86 "Bill strengthening the fight against organized crime and its financing, effectiveness and the guarantees of criminal proceedings".
87 See: law of December 12, 2005, previously analyzed.
88 Cryptologic Quaterly.

services have a considerable increase in their means of action that helps to improve the performance of equipment.

Big companies, such as Facebook, Apple, Google and WhatsApp, must allow access to authorities. These companies are not all in favor of those obligations placed on them. The company Yahoo publicly opposed it. Alex Stamos, former head of security of the company explained that if an access door was installed for the U.S. government, it could be the same for China, Russia, Saudi Arabia and other powers.

Andy Yen, co-founder of secure messaging system ProtonMail informs: "whether we like it or not, terrorists will use these tools as anyone else would. It is not because terrorists use the subway that we will close it. If we evaluate the situation rationally, the contributions to encryption to protect privacy are more important than the risk of a terrorist making use of ProtonMail. Terrorists used secret means of communication long before the existence of ProtonMail. We have not changed anything. However, what we have done is to provide to millions of people throughout the world a simple and practical way to restore their privacy"[89].

From the standpoint of the NSA, the autonomy of partners is found to be limited and second, the hegemony of the American agency is strengthened. From the perspective of non-US partners, they acede to the use, currently controlled, of technologies developed by the American military–industrial complex.

This network allows the NSA to request to the partners (who agree) to achieve politically questionable interceptions, such as those of American citizens by a third country whose laws are more lax than American laws. Furthermore, the NSA helped an Australian partner to monitor the activity of a firm of American lawyers who assisted the Indonesian state to defend itself in a dispute with Australian firms.

Mutual interests are therefore well understood but each partner is conducting its own strategy, and relations are determined by a contract[90], national sensitivities are sometimes conserved. So, when the French partners

89 ProtonMail interview: "Our objective is to reduce the cost of privacy as much as possible".
90 Memorandum of understanding.

formed an interception of underwater fibers, sessions were held in Great Britain:

> "For a whole variety of reasons, our relationships between intelligence services are rarely disturbed by national or international political conflicts. First, we help our partners to deal with what escapes their vigilance, just like they help us. Afterwards, in the majority of capitals of our foreign allies, some high-level officers, besides those of intelligence services are aware of any relationship between their intelligence services and the American NSA" [LEF 14].

The NSA has worked a lot in Germany and in the United Kingdom so that the laws protecting privacy would not put up an obstacle to their activities by intervening discreetly at the time of their planning. In France, the SUSLAF[91] maintains relations with the head of electronic intelligence. In Germany, the NSA teaches BND intelligence agents how to employ its software XKEYCORE, which facilitates the massive surveillance of the behavior of Internet users.

The safety net involves the intelligence services more than the Executive. The latter is, however, not indifferent to the situation "There are positive and negative exceptions. For example, after the election of a pro-American President, one of our European partners (author's note: it is probably France) has shown much more openness in providing us information on their own abilities and their techniques, hoping to get a better level of cooperation with us" [LEF 14]. Regarding France, cooperation in matters of intelligence is merged with military cooperation.

VI) *Surveillance does not happen only through Intelligence. The use of DNA and genetic files is becoming more frequent, even if there are discussions about it*.

On July 15, 2015, the Parliament of Kuwait passed, at the request of the government, a law prescribing to the four million Kuwaiti citizens and

91 Special US Liaison Advisor to France.

foreign residents to undergo a DNA test in order to establish a national database. The objective of this law is to facilitate the work of criminal and police investigations and to make arrests faster. This initiative followed the media coverage of a suicide bomb attack in a Shiite mosque on June 26, 2015, claimed by the Islamic State, which killed 26 people and wounded 277. In this law about the implementation of a genetic file, as in the laws that expand the powers of intelligence services and antiterrorist laws, the media-political process is the same: the exploitation of a bomb attack is supposed to justify with civil society and the international opinion the implementation of measures that violate collective and individual freedoms, while in general the measures announced were ready long ago.

Let it be observed that Kuwait is a rather sparsely populous state; this makes the implementation of a genetic file much simpler than in a State like China or even States populated by tens of millions of inhabitants. As a genetic, therefore biometric, fingerprint, the methodology is not entirely reliable. Nonetheless, the rate of false rejection or false acceptance, incidentally, very limited for the DNA, is much smaller than in a State or locality with many more citizens and residents.

Kuwait announced the establishment of a permanent committee to fight against terrorism in order to coordinate the various services of the State in this domain. Natural persons who refuse to submit to a genetic sample are liable to one year in prison, and this measure will obviously have its effects.

A genetic file corresponds to a significant economic cost. Let us not forget that some States have renounced the installation of biometric files and even biometric identification cards because of the cost, which is considered prohibitive for such measures.

Kuwait is a rich state. Although the oil windfall has lost a lot of its attractiveness, Kuwait has been able to develop its technologies and innovations in conceding considerable resources with very substantial raw materials.

Even a rich State considers that the creation of a genetic file is expensive. This is why the Members of the Kuwaiti Parliament have established an emergency fund of 400 million dollars to fund this device. Furthermore, any

Kuwaiti or any resident who refuses to allow the DNA collection risks not only a year in prison but also a 300,000 dollar fine.

Although numerous countries possess databases that keep track of the DNA of people who have been convicted of certain offenses, this law is the first in this domain to make a DNA collection for all citizens. This measure sparked controversy regarding the protection of privacy and the use that the police is able to perform with these data. Public opinion, to some extent, may be ready to accept genetic filing. Widely distributed American films have popularized the use of forensics DNA and "good common sense" comes to murmur repeatedly: "What danger is there in this process if we did nothing wrong?" and "This feature can exonerate the innocent".

But numerous legal experts' associations have expressed their reservations and this provision seems to have a "selective" future. Developing countries or emerging countries that have not developed a comprehensive course for privacy may be required, if their resources allow them, however, to install genetic centralized files with a variety of purposes, which could induce abuses.

At the moment, such a legislative provision would be impossible to be passed by the parliaments of European countries. The European Court of Human Rights prevented the United Kingdom setting up a filing of this type in 2008. The judges then ruled that maintaining DNA sampling for non-criminal offenses "could not be deemed as necessary in a democratic society"[92]. This encompassed both a disproportionate interference with the rights of plaintiffs and it was not justified in a democratic society. This jurisprudence is particularly important because the genetic file of the United Kingdom is the most significant in the world, if we refer to the size of the population. In France, the appeals of S and Marper are used for annulment before the State Council[93] commissioned by two associations against the ordinance of April 30, 2008[94] amending the ordinance of December 30, 2005[95] relating to electronic passports. What is questioned in this case, is

92 Judgment S and Marper vs. United Kingdom (appeal no. s 30562/04 and 30566/04), December 4, 2008.
93 Case no. 318013.
94 Appeal no. 2008-426.
95 Appeal no. 2005-1726.

not the fingerprints and DNA profiles, but digital fingerprints, cited in the ruling of December 4, 2008 and that are found at the center of the device from April 30, 2008. The digital fingerprints of minors may be withdrawn for biometric travel documents.

Associations address the "additional comments" to state councilors; these associations are IRIS[96], represented by their current President, Meryem Marzouki, and The League of Human Rights, represented by its President, Jean-Pierre Dubois.

The ordinance of April 30, 2008 should allow national authorities to collect and preserve the fingerprints of passport applicants[97]. The reasoning of ECHR can easily be transposed into this context, according to IRIS and LDH. The ECHR recalls that it is essential to set clear and detailed rules on the duration, storage and the use of data so that litigants are provided with sufficient guarantees[98]. These guarantees are essential when it comes to protecting personal data subject to automatic processing, especially when this information is used for police purposes. The treatments examined in the cases of S and Marper have been implemented by British authorities for the purposes of prevention, recognition, investigation and prosecution of criminal offenses. This is also the case for the retention of fingerprints under the ordinance of April 30, 2008.

It is imperative not to lose sight of the principle of proportionality. The British government believed that the data in question could be retained no matter the nature and gravity of the offenses of which the person was suspected and regardless of the age of the person involved. The ECHR emphasized the particular harm toward minors due to the importance that their integration into society holds. Retaining fingerprints as part of a treatment whose objectives are the prevention, recognition, research and prosecution of criminal offenses does not reflect a good balance between public interests and private interests. Yet, according to IRIS and the League

96 Imaginons un réseau Internet solidaire (Let's imagine a supportive internet network).
97 Article 8 of ordinance no. 2008-426 of April 30, 2008 amending article 19 of ordinance no. 2005-1726 of December 30, 2005.
98 See: Kruslin versus France, April 24, 1990, sections 33 and 35; Association for European Integration and Human Rights and Ekimdjiev versus Bulgaria, June 28, 2007; Liberty and other versus the United Kingdom, July 1, 2008.

of Human Rights, which refer to the analysis of the CNIL, the European Data Protection Controller and the group of article 29, collecting eight fingerprints, as provided in the community regulation and the conservation of these eight fingerprints in a central database are disproportionate measures while "no special measure is foreseen in parallel (...) in order to ensure the authenticity of the evidence provided to the support requests" according to the CNIL, as it is required, however, by the constitutional Council[99]. This collection is not necessary in a democratic society, to the extent where it does not seem to "be constituting in the state, a decisive tool in the fight against document fraud", in the words of the CNIL. In particular, the recollection of eight fingerprints cannot be justified in the case of minors.

Moreover, the appeal of S and Marper is full of lessons for genetic files in France.

In France, DNA profiles can be stored for 25 years after acquittal or the abandonment of prosecutions. This seems consistent with the democratic ideal to some observers, but excessive for others. No court has finally settled on the matter, but the judgment of December 4, 2008 can partially guide future doctrine currents.

The public prosecutor may order the removal of DNA profiles before the expiration of 25 years "either automatically or upon request if the conservation is no longer necessary for purposes of identification in the context of criminal proceedings". It is obvious that this removal is very rare. According to Sylvia Preuss-Laussinote[100], "In addition to the procedure open to people which not very well-known, the notion of the necessity of conservation for the purpose of identification is conceived in a very extensive manner".

The situation in France is therefore different enough from the United Kingdom. A genetic file, even if its legal objectives have expanded over the years in France, is in conformity with Article 8 of the European Convention of Human Rights and Fundamental Freedoms, Article 7 of the European Charter fundamental Rights.

The ordinance of December 4, 2008 does not concern the United Kingdom and France. Practically all developed countries or those in the

99 Constitutional council, November 15, 2007, Ord. No. 2007-557 DC, cons no. 16.
100 "Biometric data and liberties", CREDOF, December 8, 2008.

process of development have a genetic file. In order to be reliable, but also to respect the right to privacy, it is clear that national authorities must not store innocent people's samples. The principle of proportionality is taken into consideration and the requirements of democracy are not deliberately ignored. Finally, the status of minors must be subject to a thousand precautions. A child or a teenager is psychologically fragile and storing their fingerprints, whether digital or genetic ones, is an obstacle to a smooth integration into civil society. However, these rules are increasingly difficult to control. Public authorities and particularly the State show a desire for security. They believe that the storage of genetic samples, including those of innocent persons, may prevent crimes and serious offenses. Additionally, some manufacturers achieve substantial gains with genetic fingerprint sampling. The people involved, with the exception of associations defending human rights, are in support of easy sampling and sometimes in support of the indefinite retention of genetic samples. The situation is, nevertheless, highly evolutionary and the law of July 2015 in Kuwait can be emulated in other regions of the world.

Conclusion

Players are in close symbiosis with security, whether it involves States or businesses. The different levels of analysis are legal, geopolitical and economic.

Concerning the States, defense and security are national because they do not apply solely to military defense but rather to all responsible administrations of essential resources.

Resilience implies the willingness and the capacity of a country, the society and public powers to resist the consequences of an abuse; it also involves public authorities, economic players and the civil society as a whole. This leads to the establishment of priorities in the deployment of competences of intelligence, analysis and decision-making. This resilience also involves a collaboration between States and private companies in strategic domains.

The doctrine of national security appeared in the United States at the time of a bipolar world, although if it should be noted that before the "big stick" of Th. Roosevelt[1], it also took place in Latin America by combining the "external" enemy and the "internal" enemy, which justified the use of Brazil, Argentina and other States of scientific tortures, contrary to human rights, which had, nevertheless, served as an ideological substructure to the Western bloc in its struggles against the Soviet bloc. After the collapse of the

1 1904.

Security and Privacy in the Digital Era, First Edition. Claudine Guerrier.

Soviet bloc, the United States remains an omnipotent military power, yet China and India's economic boom has not yet been accompanied by a similar military development equivalent to their economic and financial development. NATO plays an increasingly important part. The old states of Central and Eastern Europe have joined NATO. France and the United Kingdom, after the loss of their colonies, have remained military powers. France, for several decades, while remaining an active member of the Atlantic alliance, left the integrated military organs and led a relatively independent security policy. This is no longer the case. France formally adopted the doctrine of national security[2]. Under the leadership of Nicolas Sarkozy and François Hollande, France, through the partnership of the above-mentioned intelligence, approached the United States and returned to the integrated military structures of NATO. However, France continues to fulfill a significant military role, as an intervener, like other countries, particularly the United Kingdom in Afghanistan, and then playing a supplementary card in the Western interventions in Africa (Mali and Central African Republic). The European Union, an economic power, is not a military power even if it starts to play a significant diplomatic role, as it appeared to in the frozen conflict between the West and Russia of the 21st Century, including the support given to Ukraine and the economic sanctions imposed on this Eastern power. However, currently, the security of Europe is still provided by NATO, the United States, more reticent, and the two nuclear states of the European Union, the United Kingdom and France, which despite the privileged alliance with the United States on almost all territories, of Libya in the Middle East, continue to play a part in national failures, although somewhat subtle, with failures and successes.

Borders have not changed much since World War II, although it is obvious that the borders inherited from the colonial era are involved in tribal wars, and ethnic ones in Africa. In Europe, Czechoslovakia decided by democratic vote, to be broken apart into two states, and the former Yugoslavia has been the subject of wars in which the UN and NATO appeared to halt the Serbian advance supported by Russia.

These States proceeded to set up partnerships between intelligence services, as has been explained above, and the military–industrial complexes

2 French White Paper on National Security, 2008–2009, related to the doctrine of national security.

have led to productive collaborations in the United States, but also in other less important but significant powers.

In particular, during this period, military drones have demonstrated their effectiveness in Iraq and Pakistan. Let us recall that the main industrial sectors in terms of drones are located in the United States, once again, but also in Israel, which proved its strategic skill in the majority of sectors where resilience is requested. The sources of law have been adapted to the security needs, in intelligence, within international and regional organizations.

Another key player in social control is business. All businesses, large, medium or small have made significant profits by conducting the transfer of personal data files; these files are privileged elements of flow from within boundaries or beyond boundaries. The law of the European Union, since instruction 95/46, requests an equivalent level of protection in the matters of transfers of personal data. The vicissitudes that accompanied the negotiations between the United States and the European Union[3] have translated the necessary balance between the principle of free trade and its requirements, quite significant within the European Union in order to protect personal data, even when it is sold to States that do not have the same degree of discipline that Europe has in the domain of respect for privacy.

Over the Internet, indexing was also a source of substantial profits for some technological and economic operators. The required deindexation demanded by the right to oblivion since the Google Spain ruling has introduced a new dimension for commercial companies and the debate remains in progress.

Finally, let us not forget that the Internet allows us, under the principle of neutrality, to track in a temporal dimension individuals and businesses at every moment.

With regard to the biggest companies, a complex relationship has been established between intelligence agencies and the servers employed by Google, Apple, Facebook and other operators. Some recent laws have demanded the reporting of data and metadata to public authorities. This

3 Safe Arbor Principles and invalidation by the European Court of Justice, dated October 6, 2015.

corresponds to a financial loss for companies. Some of them protested against the "repressive" role that was assigned to them. In some countries[4], intelligence agencies have a direct or indirect access to servers and these companies participate in the operation of massive data collection over the Internet. In the United States, as of 2013 and 2104, companies have expressed harsh criticisms of the way the government collects information. Google, Apple, Microsoft, Facebook, Twitter, AOL and Yahoo requested that government intelligence agencies are no longer able to obtain metadata in relation to Internet users.

Indeed, in the United States, Canada and France, if government authorities are not authorized to collect information in relation to certain users, notably legal entities governed by public or private law, they have access to certain metadata. These requests were not echoed by the legislator, and numerous metadata in Western states are collected and analyzed by governments. Certainly, recalcitrant operators are theoretically entitled to leave the territories where these legislations apply, but it is hardly an option for the majority of these operators. The consequences of this situation established by the sources of law are both financial and political. It is obvious that institutionalization of these metadata recollections is in progress and the evolution is not ready to be reversed.

Transparency cannot be the keyword for the intelligence agencies, including their relationships with companies that are often multinational companies and that have significant financial and economic power instruments. Nevertheless, the history of relations between governments and these companies that collect metadata should be followed with caution.

Therefore, in June of 2015, before the vote on the new law, GHCQ, the British intelligence agency, was sentenced by a court for having kept data intercepted from two non-government organization (NGOs) for too long: GCHQ was sentenced due to having violated the rules it had laid down. The British intelligence agency often performs, like its counterparts, data capture. These procedures are validated by several Commissioners and by the Parliamentary Intelligence and Security Committee. For data collection, however, the GCHQ operates according to its own regulations,

4 See: supra.

which it does not always respect scrupulously. The Investigatory Powers Tribunal (IPT) declared the retention period of intercepted data to be illegal in the case of the Egyptian Initiative for Personal Rights and the South African non-profit Legal Resource Centre. In these two instances, the IPT found that there had not been a lack of proportionality, but that the data were stored for longer than it had been anticipated by the agency itself.

If the partnership between intelligence services generally works well, some contradictions may arise between certain interests. This is how the economic surveillance carried out by the United States can rely in some cases on a national cooperation. In particular, Deutsche Telekom, assisted by the German secret service of the Bundesnachrichtendienst (BND), captured the communication flow of France Telecom on behalf of the National Security Agency (NSA). Airbus, Eurocopter and France Telecom are identified targets of the NSA collaborating with the BND, as revealed by "Le Monde", who accessed the documents of the Committee of Inquiry of the Bundenstag. With the efficient help of Deutsche Telekom, with whom the German intelligence services have signed a memorandum of understanding, the BND installed a surveillance of the "flow of communications managed by France Telecom passing through Germany" since 2005. Many other agreements of the same kind probably exist and have not been made public. But it is obvious that the economy moves the geopolitics and vice versa. The company players continue to actively participate in these information and trade through flows.

The last players are the human and citizen rights advocacy organizations. Advocacy organizations for human rights, notably in the United States and United Kingdom, even if they act discreetly with regard to the adoption of certain laws, have denounced violations of privacy and have appeared before courts, attaining some success, in both the United States and United Kingdom. In France, when adopting a state of emergency of 3 months on November 19 and 20 of 2015 by the Senate, the League of Human Rights and other NGOs expressed their reservations in relation to what can appear to be a disproportionate restriction in time and space for individual and collective freedoms. The tribunitian function is certainly more reliable for those NGOs that act before the courts, because the American or British legislator takes initiatives if appeals are able to inflict a blow, including insignificant ones with regard to the construction implemented since the beginning of the 21st Century. These NGOs are bearers of petitions,

warnings related to the respect for privacy and the necessary consideration of new aspects of privacy with the convolutions relating to the Internet, digital sphere and security in all its forms.

Citizens are all involved in the challenges of social control that apply to them. They are aware of being under constant surveillance through geolocation and the Internet. Accustomed since childhood to various aspects of political and economic security, they are acculturated to the legitimation, and even to the legitimacy of social control. All citizens of Western countries check their e-mail on their mobile phone even outside working hours. They are almost always connected, including through their objects.

However, differences are emerging between these citizens. Some have adopted the word of media order "I don't care about surveillance because I have nothing to hide!". Big Brother is not a threat to them. Other people are selective with regard to the modalities of social control: they sometimes accept biometric palm recognition for access to their canteen or workplace, but they do not hesitate to complain if they are subject to constant monitoring through video surveillance in their workplace. They may become indignant of the excesses of certain laws that increase the possibilities of interception or the collection of metadata. Finally, a small minority of citizens is adept at activism, is hostile to various forms of social control, refuse withdrawals of their DNA, proclaim their hostility to "all security", sign petitions, if it allows a Supreme Court referral, who will be able to address some provisions that violate individual and collective freedoms. Sociologists have worked on these fields of investigation, even if there is no real statistical distribution regarding the attitudes of different citizens against differentiated and (or) converged controls. "...a fear is buried deep within men, but it is erased for a time of memories, it reappeared in the form of a feeling of insecurity"[5].

In the parliamentary precincts, when laws justify "the security exception", few of the population's representatives even deign to speak out against the damage caused to individual and collective freedoms.

Thus, when in France, in November of 2015, the state of emergency was extended for a period of 3 months, there were only six members of

5 Sebatian Roché, "The feeling of insecurity" Today's sociology, PUF, Paris, 1993, p. 136.

parliament[6] who delivered a vote against. More interesting is the unanimity of the vote of the Senate[7] that allows large mass media to caption "unanimous vote", and, in smaller letters, "votes cast".

The lessons of Jacques Ellul have a more significant scope for the 21st Century than for the 20th Century. However, there is a huge concern that social control is more and more frequently regarded as a standard, regardless of the issues considered:

> "The propagation of fear has facilitated the extension of the precautionary principle of natural or technological risks toward crime, to the point of justifying, almost without public protest, the empowerment of dangerousness, arbitrary blacklisting, black sites scandals and torture…" [DEL 13].

The former president of the CNIL stated that "this all-traceable society is becoming a nightmare, but if we do not establish strong safeguards today, it will soon be too late"[8]. But the worst is not always sure.

With Mireille Delmas-Marty [DEL 13], we can suggest "In the face of the BenLaden/Big Brother alliance, the best answer in 'this massive uprising of the imagination' is probably what the poet Edouard Glissant calls "the thought of the earthquake: a thought that is neither fear nor weakness, but the assurance that it is possible to approach this chaos, to endure, and grow in the unpredictable" [GLI 05].

Next to Mireille Delmas-Marty, let us reflect on this sentence that seems to be able to serve as a provisional conclusion to this essay: "The State that claims to eradicate any insecurity, even a potential one, is caught in a spiral of exception, suspicion, and the oppression that can go up to the point of disappearance of liberties, more or less complete" [DEL 13].

6 And one abstention.
7 Twelve abstentions.
8 Alex Türk, "The awakening will be very painful", Libération, March 28--29, 2009.

Bibliography

[ALI 10] ALIX J., *Terrorisme et droit pénal, Etude critique des incriminations*, Dalloz, Paris, 2010.

[CHE 13] CHEMILLIER-GENDREAU M., *De la guerre à la communauté universelle*, Fayard, Paris, 2013.

[COD 15] CODACCIONI V., *Justice d'exception, l'Etat face aux crimes politiques et terroristes*, CNRS Editions, Paris, 2015.

[DEL 13] DELMAS-MARTY M., *Libertés et sûreté dans un monde dangereux*, Le Seuil, Paris, 2013.

[ELL 12] ELLUL J., *Le système technicien*, new edition, Le Cherche-Midi, Paris, 2012.

[FOU 75] FOUCAULT M., *Surveiller et punir*, Gallimard, Paris, 1975

[GLI 05] GLISSANT E., *La Cohée du Lamentin. Poétique V*, Gallimard, 2005.

[GRA 11] GRANGER M.-A., Constitution et sécurité intérieure, Essai de modélisation juridique, LGDJ, Paris, 2011

[GUE 00] GUERRIER C., *Les écoutes téléphoniques*, Editions du CNRS, Paris, 2000.

[HAN 08] HANNOUN C., "L'impact de la financiaristion de l'économie sur le droit du travail", *RDT*, 2008.

[HER 97] HERMET G., *L'Espagne en 1975, évolution ou rupture*, Fondation nationale des sciences politiques, 1997.

[LAT 00] LATOUR B., "La fin des moyens", *Réseaux – Communication – Technologie – Société*, vol. 18, no. 100, p. 39, 2000.

[LEF 14] LEPEBURE A., *L'affaire Snowden, comment les Etats–Unis espionnent le monde*, La Découverte, 2014.

Security and Privacy in the Digital Era, First Edition. Claudine Guerrier.

[MAT 14] MATTELART A., VITALIS A., *Le profilage des populations*, La Découverte, Paris, 2014.

[ROC 93] ROCHÉ S., *Le sentiment d'insécurité, Sociologie d'aujourd'hui*, PUF, Paris, 1993.

[SOL 09] SOLZHENITSYN A., *In the First Circle*, Harper Perennial, 2009.

[WAR 11] WARFMAN D., *Private Security in France*, PUF, 2011.

Index

A, B, C

D, E, F

Security and Privacy in the Digital Era, First Edition. Claudine Guerrier.

G, H, I

J, K, L, M

N, O, P

R, S

T, U, V

Other titles from

in

Innovation, Entrepreneurship and Management

2016

BARBAROUX Pierre, ATTOUR Amel, SCHENK Eric
Knowledge Management and Innovation (Smart Innovation Set – Volume 6)

BOUTILLIER Sophie, CARRÉ Denis, LEVRATTO Nadine
Entrepreneurial Ecosystems (Smart Innovation Set – Volume 2)

GALLAUD Delphine, LAPERCHE Blandine
Circular Economy, Industrial Ecology and Short Supply Chains (Smart Innovation Set – Volume 4)

MEGHOUAR HICHAM
Corporate Takeover Targets

MONINO Jean-Louis, SEDKAOUI Soraya
Big Data, Open Data and Data Development (Smart Innovation Set – Volume 3)

MOREL Laure, LE ROUX Serge
Fab Labs: Innovative User (Smart Innovation Set – Volume 5)

2015

CASADELLA Vanessa, LIU Zeting, DIMITRI Uzunidis
Innovation Capabilities and Economic Development in Open Economies (Smart Innovation Set – Volume 1)

CORSI Patrick, NEAU Erwan
Innovation Capability Maturity Model

CORSI Patrick, MORIN Dominique
Sequencing Apple's DNA

FAIVRE-TAVIGNOT Bénédicte
Social Business and Base of the Pyramid

GODÉ Cécile
Team Coordination in Extreme Environments

MAILLARD Pierre
Competitive Quality and Innovation

MASSOTTE Pierre, CORSI Patrick
Sustainability Calling

MASSOTTE Pierre, CORSI Patrick
Operationalizing Sustainability

2014

DUBÉ Jean, LEGROS Diègo
Spatial Econometrics Using Microdata

LESCA Humbert, LESCA Nicolas
Strategic Decisions and Weak Signals

2013

HABART-CORLOSQUET Marine, JANSSEN Jacques, MANCA Raimondo
VaR Methodology for Non-Gaussian Finance

2012

DAL PONT Jean-Pierre
Process Engineering and Industrial Management

MAILLARD Pierre
Competitive Quality Strategies

POMEROL Jean-Charles
Decision-Making and Action

SZYLAR Christian
UCITS Handbook

2011

LESCA Nicolas
Environmental Scanning and Sustainable Development

LESCA Nicolas, LESCA Humbert
Weak Signals for Strategic Intelligence: Anticipation Tool for Managers

MERCIER-LAURENT Eunika
Innovation Ecosystems

2010

SZYLAR Christian
Risk Management under UCITS III/IV

2009

COHEN Corine
Business Intelligence

ZANINETTI Jean-Marc
Sustainable Development in the USA

2008

CORSI Patrick, DULIEU Mike
The Marketing of Technology Intensive Products and Services

DZEVER Sam, JAUSSAUD Jacques, ANDREOSSO Bernadette
Evolving Corporate Structures and Cultures in Asia / Impact of Globalization

2007

AMMI Chantal
Global Consumer Behavior

2006

BOUGHZALA Imed, ERMINE Jean-Louis
Trends in Enterprise Knowledge Management

CORSI Patrick *et al.*
Innovation Engineering: the Power of Intangible Networks

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.

INNOVATION AND TECHNOLOGY SET

Coordinated by Chantal Ammi

"The state, that must eradicate all feelings of insecurity, even potential ones, has been caught in a spiral of exception, suspicion and oppression that may lead to a complete disappearance of liberties." (Mireille Delmas Marty, Libertés et sûreté dans un monde dangereux, 2010)

This book will examine the security/freedom duo in space and time with regards to electronic communications and technologies used in social control. It will follow a diachronic path from the relative balance between philosophy and human rights, very dear to Western civilization (at the end of the 20th Century), to the current situation, where there seems to be less freedom in terms of security to the point that some scholars have wondered whether privacy should be redefined in this era. The actors involved (the Western states, digital firms, human rights organizations etc.) have seen their roles impact the legal and political science fields.

Claudine Guerrier is Professor of Law at the Institut Mines-Télécom and the Télécom Ecole de Management in Paris, France. Her research focuses on the tense relationship between technology, security and privacy.

ISTE
www.iste.co.uk
WILEY
9 781786 300782