# Personal data and cyber-surveillance

Me Cécile Doutriaux
*Lawyer and member of the Cyber-Defence and Cyber-security Chair of the Saint-Cyr Coëtquidan schools.*

*December 2014 - Article III.17*
***This article was first published in the December 2014 RDN - n° 775.***

New technologies increase the surveillance capacities and the potential intrusions in the life of citizens (1). M. Edward Snowden, former employee of the CIA (2), made public in 2013 (3) some secret information from the American National Security Agency (4) and revealed the American government Prism, XKeyscore, Boundless Informant and Bullrun surveillance programs as well as the British government Tempora, Muscular and Optic Nerve programs. This major espionage of the personal data of world citizens would supposedly be justified by the fight against terrorism, notably by the Patriot Act in the United-States. Many countries, such as Germany, France, Spain and Brazil expressed outrage (5) at the NSA practices on the pretext that these actions would be a cause for suspicion, detrimental to good relations of trust between nations. However, cyber-surveillance of citizens is not a new practice, exclusive to the United-States for even if the surveillance means of "Five Eyes" (6) are huge, the European Union is not inactive and intercepts personal data too (7) .

The reality of cyber-espionage puts into question the trust placed by citizens in governmental authorities, responsible for guaranteeing the confidentiality of electronic correspondence and the protection of personal data, keeping in mind that according to the law "computer science must be at the service of each citizen and must not interfere with privacy or individual or public freedom"(8) **.**

(1) Éric Denécé "the control and coordination of intelligence activities", January 2013.
(2) The purpose of the National Central Intelligence Agency created in 1947 is to obtain underground intelligence in order to ensure the security of the national territory, in accordance with the instructions from the President of the United States or the Director of National Intelligence.
(3) Notably through the Washington Post on 9 June 2013 published by Barton Gellman, Aaron Blake and Greg Miller and by the Guardian on 17 June 2013.
(4) The National Security Agency (NSA) is a governmental organisation from the United-States Department of Defence, responsible for the Signals Intelligence, the security of information systems and the processing of the American government data.
(5) The Express 18 December 2013.
(6) Alliance between the United-Kingdom, the United-States, Canada, Australia and New-Zealand for intelligence needs.
(7) See newspaper « Le monde » of 20 March 2013 http://www.lemonde.fr/international/article/2014/03/20/les-services-secrets-britanniques-ont-acces-aux-donnees-des-clients-francais-d-orange_4386266_3210.html.
(8) First Article 1er of the law on privacy, data protection and freedom of information from 1978.

## I. National and international protection of personal data and of the confidentiality of electronic correspondence.

The sources of data have become extremely diversified and the data is no longer only collected and stored by administrations and companies, but also put online by people themselves. This reality implies protecting this personal data and the protection established by the law varies according to the type of data (personal (9), sensitive (10) and connection (11))

The connection data is especially targeted by cyber-espionage and like the IP address, they are considered personal data and are protected by the law protecting privacy (12) such as that recognized by article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (13).

Several States (14) have produced national protection laws for personal data, as is the case in France with laws on privacy, data protection and freedom of information from 6 January 1978. These national laws set the basic principles of data protection, such as confidentiality and the deletion of data at the expiry of the prescribed period for their storage. The data is also protected at the European level. Thus, the purpose of the Convention n°108 of the Council of Europe of 1981 (15) is to guarantee, on the territory of each State, to each physical person the respect of his or her privacy in the automatic processing of his or her personal data. Article 5 of Directive 2002/58/CE establishes that the cybernaut must be informed of all collecting of information, that he has a right to know the reason of the collection of data and to oppose it (16). The older Directive 95/46/CE (17) has an overall regulatory approach in order to protect the European citizens' personal data and ensure free movement of data throughout the European Union. It considers that any gathering of personal data must be licit, fair and not excessive in view of the purposes to be achieved.

This protection of personal data is completed by the confidentiality of electronic correspondence, recognised by many national and international texts such as articles 12 from the Universal Declaration of Human Rights in 1948 ( 18),

(9) Are information about a physical person, identified or who can be identified, directly or indirectly, by reference to his or her specific features, such as names, surnames, addresses (physical and electronic), telephone number, place and date of birth, social security number, digital prints, DNA, etc.... they may be collected and stored, with the possibility for their owners to make use of the right to access and modify.

(10) Sensitive personal data show racial or ethnical origins, political, philosophical, religious, relative to health or sex life opinions, and may not be collected, except if the person in question has given express consent.

(11) Connection data, allow the identification of the subscriber of a contract, from a phone number or an IP address and can be collected under conditions strictly defined by law.

(12) In France, the right to privacy is guaranteed by article 9 of the Civil Code.

(13) Article 8 « Everyone has the right to respect for his or her private and family life, home and communications ».

(14) Notably Belgium, Iceland, the Netherlands, Spain and Switzerland with for example, the Swiss federal law on data protection from 19 June 1992 http://www.admin.ch/opc/fr/classified-compilation/19920153/201401010000/235.1.pdf consulté le 05/09/2014.

(15) Convention n°108 from the Council of Europe from 28 January 1981 for the protection of persons regarding the automatic processing of personal data, established on the basis of relevant work founded by the OCDE and four non-European member States (Australia, Canada, Japan and United States).

(16) "The member States guarantee that the use of electronic communication networks for the purpose of storing information or accessing information stored in a subscriber or a user's terminal equipment is possible only if the subscriber or user, in accordance with Directive 95/46/CE has clear and complete information amongst other things as to the purposes of the processing and if the subscriber or user has a right to refuse said processing by the person in charge of the data processing".

(17) Directive 95/46/CE of the European Parliament and the Council from 24 October 1995 relating to the protection of physical persons with regards to the processing of personal data and the free movement of said data, Journal officiel n° L 281 from 23/11/1995 p. 0031 - 0050

(18) Article 12: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks »

8 from the European Convention on Human Rights in 1950 (19), 17 from the International Covenant on Civil and Political Rights in 1966 (20), by article 37 of the Constitution of the International Telecommunication Union in 1992 (21) but also by the Directive in the European Union on the Telecommunication Field in 2002, in article 5 (22). In France, the confidentiality of correspondence is ensured by article L.241-1 from the internal security code (23) and article 226-1 from the Penal code protects the citizens' private life (24).

Despite all of these measures, major quantities of personal data from European and American citizens are gathered by the States' Intelligence departments.

## II. Is the cyber-surveillance of citizens' data by the United States legal?

The necessity of ensuring national security enables the United-States to use exceptional powers, which can limit the protection to which citizens are entitled. Are these measures, derogating from the principle of personal data protection and correspondence privacy, legal?

A distinction must be made between intelligence collected by open and authorised means, namely through security inspections, and those obtained though covert means, which is to say espionage.

### A. Is the covert collection of data such as that undertaken by the States licit?

Though espionage in times of war is authorised and defined by article 29 of the Hague Regulations of 1907 (25), there is no definition for espionage in times of peace, and to date, there is no international convention to regulate electronic espionage activities between States, in spite of their massive increase.

Hence, undisguised soldiers entering the operations area of the enemy army, for the purpose of collecting information, are not considered spies".

(19) Article 8 of the CEDH: "Everyone has the right to the protection of his privacy, family, home or correspondence".

(20) Article 17 of the International Covenant on Civil and Political Rights: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks »

(21) Article 37 of the Constitution of the International Telecommunication Union: «The member States are committed to taking every possible measure, compatible with the telecommunication system used, in order to ensure the privacy of international correspondence"

(22) Article 5: "The member States guarantee, by national law, the privacy of communications made through a public communication network and electronic communication services available to the public, as well as the privacy of the related traffic data. In particular, they forbid any other person than the users to listen, intercept, store the related traffic communications and data or to submit them to any other interception or surveillance mean, without the consent of the users in question, except when this person is legally authorised to do so".

(23) Article L241-1: "The privacy of correspondences transmitted by means of electronic communications is guaranteed by law. This right may only be impaired by public authority, only reasons of public interest alone as provided for by the law and within its limits."

(24) Article 226-1 of the Penal Code : "The act of deliberately invading the privacy of others, by any process, is punishable by a year's imprisonment and a fine of 45,000 euros."

(25) Article 29: « Only the person who, by acting in a clandestine manner or under false pretexts, in order to collect or try to collect information in the operation zone of a belligerent, with the intention of communicating them to the adverse party, can be considered a spy »

However, does an act of espionage represent a violation of international law, which might incur the States' liability? In reality, the responsibility of the State, because of the activity of their secret services, doesn't give rise to much in the way of legal developments, as these cases call for low-key resolution, through direct or diplomatic negotiations and the sanction is even more inconceivable as this practice is established and mutual between States. Thus, in espionage cases, the States prosecute the intelligence agent before national courts, without undertaking any form of repressive action against the State sponsor. Thus, in France, the intelligence agent can be tried before national courts, on the basis of article 702 of the Code of Criminal Procedure (26) if he has understandings with a foreign power (27) and delivers computer data (28) which, if disclosed, could be of a nature likely to be detrimental to the basic interests of the nation (29). Of course, the agents guilty of cyber-espionage can be prosecuted for intrusion into computer systems on the basis of article 323-1 of the Criminal Code (30), the sentence being majored when the attack is made against an automated processing system implemented by the State (31). Trying the agent was the option chosen by the United-States on 19 May 2014 when choosing to prosecute five Chinese soldiers accused of cyber-espionage for unauthorised access to computers and the spreading of computer viruses (32).

Does this mean that no sanction can be applied against the State itself for its acts of cyber-espionage? A State has sovereignty on its territory which allows it to secure its borders from any external influence, but which also compels it to respect the other States' sovereignty. Hence cyber-espionage would constitute grounds for liability of the States, in the case of simultaneous violation of territorial integrity, which constitutes a casus belli according to article 2 of the United Nations Charter (33). However, in terms of territoriality, it is difficult to precisely set the borders of cyber-space and the access to data or computer systems is made "remotely" by the intelligence agent, through spyware for example, so that there is no real violation of the territorial integrity of the State. This situation makes the repression of cyber-espionage, such as those conducted by the States in times of peace, ultimately purely hypothetical and the outraged public declarations made by the heads of States on this subject are more directed at limiting the outrage of the citizens than aiming for a breakdown in international relations.

(26) In times of peace, the crimes and offences against the basic interests of the nation are investigated and heard by courts of general jurisdiction (Assize Court, Criminal Court) and according to the rules of the Criminal Code, when the prosecuted facts are considered a crime or an offence punishable under articles 411-1 to 411-11 of the Criminal Code.

(27)Article 411-5 Criminal Code: "The act of having understandings with a foreign power, with a foreign company or organisation or under foreign control or with their agents, when it is liable to be detrimental to the basic interests of the nation, is punishable by ten years of imprisonment and a 150,000 euro fine.

(28) Article 411-6 Criminal Code: « The fact of delivering or making accessible to a foreign power, a foreign company or organisation or under foreign control or to their agents, any process, object, documents, computer data or files which, if exploited, disclosed or gathered is liable to be prejudicial to the basic interests of the nation, is punishable by fifteen years of criminal detention and a 225,000 euro fine».

(29) Article 410-1 Criminal Code: « The basic interests of the nation are understood as being its independence, its territorial integrity, its security, the republican form of its institutions, its means of defence and diplomacy, the protection of its people in France and abroad, the balance of its natural habitat and its environment and the key elements of its scientific and economic potential and its cultural heritage. ».

(30) Article 323-1 of the Criminal Code: « The fact of accessing fraudulently in a part or all of an automated data processing system is punishable by two years of imprisonment and a 30,000 euro fine and intrusions against the State's computer systems is more severely punishable by five years of imprisonment and a 75,000 euro fine ».

(31) When the result is either the deletion or the modification of the data held on the system, or degradation in the operation of said system, the sentence is three years of imprisonment and a 45,000 euro fine. When the offences have been committed against an automated personal data processing system implemented by the State, the sentence is increased to five years of imprisonment and a 75,000 euro fine.

(32) Daniel Ventre, Chinese soldiers wanted by the FBI for economic espionage. Econflicts blog, http://econflicts.blogspot.fr/2014/05/des-militaires-chinois-recherches-par.html, 21 mai 2014.

(33) Article 2 of the United Nations Charter: "The States must refrain from the threat or use of force against the territorial integrity or political independence of any State.

## B. Authorised cyber-surveillance by the interception of telecommunications and collecting connection data

Interference with the privacy of citizens by the State is possible, but must be well found in fact (34) and provided accessible legislation, foreseeable and relatively comprehensive, in order to offer guarantees to the people affected by cyber-surveillance in democratic societies (35).

In order to answer to their citizens for the accusations of massive espionage, the United-States declared they had acted on the basis of the Patriot Act, a set of security laws voted in reaction to the 11 September 2011 attacks and designed in such a way to enable the American Intelligence services to access data stored in the servers of American companies, including companies the United-States. In order to address the terrorist threat, arrangements were also made in Europe to break electronic correspondence secrecy in the case of major threats, in reaction to the terrorist attacks on Madrid on 11 March 2004 and in London on 7 July 2005. Indeed, the European Union (36) allows the collecting of connection data and Directive 2006/24/CE (37) states that telephone operators and Internet access providers must retain all data enabling them to identify the cybernauts, as well as locating them and being able to know the time and date of their communications, for a time ranging between six and twenty-four months, depending on the countries' national laws (38).

In France, two distinct and complementary mechanisms make it possible to monitor the citizens' electronic communications. One of them is based on article L. 241-2 of the internal security code (39), the other one based on article L.34-1-1 of the Postal and Electronic Communications Code (40). The reasons put forward in order to justify this surveillance of networks and electronic communications are the safeguarding of national security 41, the fundamental interests of the nation and the fight against terrorism.

(34) European Court of Juman Rights, Janowiec and others vs Russia [GC], nos 55508/07 and 29520/09, §§ 213-214, 21 October 2013.

(35) Report from the Research Directorate of the European Court of Human Rights, national security and European jurisprudence 2013.

(36) The European union is a regional organisation, based upon a treaty which manages the economic and political cooperation between its 28 member States, namely Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Estonia, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxemburg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, the United-Kingdom and Croatia.

(37) European directive 2006/24/CE relating to the retention of data generated or processed within the framework of the supply of electronic communication services accessible to the general public or public communication networks.

(38) The length of time the connection data is to be stored is of one year for France and Belgium, and one month for Germany.

(39) Article L.241-2 of the internal security Code: the interception of correspondence issued through electronic communications for the purpose of searching for national security-related information, safeguarding key elements of the scientific and economic potential of France, or the prevention of terrorism can be exceptionally authorised.
Article L.244-2 of the security code: The Minister of Defence or the Minister of Home Affairs can obtain from physical or moral people operating the electronic communications networks or electronic communications services providers, the necessary information or documents in order to realise and operate the interceptions authorised by the law.

(40) Article L.34-1-1 of the Postal and electronic communications Code: In order to prevent terrorist acts, the duly authorised officials of the police and national police services can require the operators to supply the technical data relating to the identification of the subscription or connection numbers to electronic communications services, to the inventory of all the subscription or connection numbers of a designated person, to the data relating to the location of the terminal equipment used, to the technical data relating to the communications of a subscriber concerning the list of incoming and outgoing calls, the date and duration of communications. The application of this article has been extended to 31 December 2015.

As such, the telephone operators and Internet access providers are required to keep the connection data of their users during one year in France and make them available to the authorities, in conformity with article 34-1 of the Postal and electronic communications Code (42).

What's more, since the Act on Military Programming n°2013-1168 on 18 December 2013 ( LPM ), the article L. 246-1 of the internal security code (43) authorises the collection of information processed or stored by networks and connection data related to the identification of the subscription numbers, the locating of the equipment used as well as the communications of a subscriber. In fact, the act on military programming would unite all of the provisions of the 1991 act on security interceptions and those of the anti-terrorist law of 2006 on collecting connection data.
These measures, restricting the right to privacy and the protection of personal data, were provided for by article 8 paragraph 2 of the European Convention for the Protection of Human Rights and Fundamental Freedoms which mentions that a public authority may only interfere with the exercise of the right to privacy if this interference constitutes a measure necessary for national security. There is therefore a limit to the right to privacy, anticipated in the texts, in so far as public interest must take precedence over personal interest, since it is above all a question of sustaining the cohesion of society as a whole. Consequently, the cyber-surveillance of the citizens' data, expressly provided for by the texts, is perfectly legal at a national, European and international level.

**Even if exceptional rules are accepted, do these measures give full authority to the States?**

Though national security considerations can impact the guarantees offered to the citizens by national and international laws, the need to fight terrorist criminality provides no justification for an indefinite extension of security interceptions, and limits are set in order to prevent abuses. Indeed, only public authority may infringe upon electronic correspondence privacy, in exceptional circumstances, only for reasons of public interests such as provided for and within the limits set by the law. (44)
The power to secretly monitor citizens is tolerable only if the means provided for in the legislation are acceptable in a democratic society. The European Court of Human Rights has specified the limits to these exceptional measures in several case rulings. For example, in the Klass and others vs Germany case (45), the ECHR specifies that the States do

(41) Article L1111-1 of the Defence Code: «The purpose of the national security strategy is to identify the full range of threats and risks likely to affect the life of the Nation, notably regarding the protection of the population, the integrity of the territory and the permanency of the institutions of the Republic.

( 42) Article L34-1 (modified by LAW n° 2013-1168 of the 18 December 2013 - art. 24 ) For purposes of researching, identifying and prosecuting criminal offences or for the needs of preventing the violation of automatized data processing systems such as provided for and punishable by articles 323-1 to 323-3-1 of the Criminal Code, and for the sole purpose of providing for judicial authority or national information security systems authority referred to in article L. 2321-1 of the Defence code (OIP – Prime minister) deferred for a period which shall not exceed one year to the operations aiming to delete or render anonymous certain categories of technical data.
(43)Article L. 246-1 of the code on internal security: For the purposes listed in article L. 241-2, the collecting of information or documents processed or stored by their networks of electronic communications services, including the technical data related to the identification of subscription connection numbers of a designated person, t the location of the terminal equipment used as to the communications of a subscriber concerning the list of outgoing and incoming numbers, the duration and date of communications. This article took effect on the 1st of January 2015.
(44) According to article L.241-1 of the code on internal security.
(45) Klass and others vs Germany case (application n o 5029/71) judgement of 6 September 1978.

not have unlimited latitude in subjecting citizens to secret monitoring measures, in the name of the fight against terrorism. In the Leander vs Sweden (46), the Court recalled that state interference in the private lives of its citizens must meet a pressing social need and be proportionate to the legitimate purpose. Lastly, the power to order measure for the secret monitoring of citizens is permissible only if it is strictly necessary to the preservation of democratic institutions, which in practice means that there must be adequate and effective guarantees against abuses. Therefore it is not enough to invoke the laws to justify the massive surveillance of the citizens' data, any misuse must be punishable, and independent or legal administrative authorities must be in charge of controlling. In France, there are two independent administrative authorities, the National Commission for Data Protection and Liberties (CNIL), in charge of ensuring respect of privacy and liberties in the digital world and the National Commission for the Control of the Security Interceptions (CNCIS) in charge of verifying the lawfulness of the security and communications technical data interceptions. The CNIL has power to control and to sanction (notably financially), whereas the CNCIS is mostly responsible for ex-post control and addressing recommendations to the ministers, without really having any enforcement power.

(46)Leander vs Sweden case (application n o 9248/81) judgement of 26 March 1987.

## III. Are cyber-surveillance measures proportionate and legitimate or do they challenge the rule of law?

The protection of national security is a legitimate target which can entail restrictions on the respect of privacy, however cyber-surveillance measures must be proportionate to their purposes. Yet according to E. Snowden, « Most people in developed countries use the Internet and the States use this to secretly expand their powers, beyond what is necessary and appropriate ».