# Encryption, security and liberties

## Position of the “Observatoire des libertés et du Numérique”, january 2017

# Position summary

**In the digital age, legal and technical surveillance capabilities of States have become so advanced that fundamental right to privacy, cornerstone of freedoms of expression, opinion and information, has been challenged lately in France as well as throughout the world.**

**As such, the capability of encrypting digital communication and data is mandatory in order to preserve fundamental rights and liberties. Encryption remains one of the last barrier against arbitrary and illegal intrusions, either from States, the private sector or criminals.**

**However, encryption goes far beyond human's right concerns: since digital technologies are now a part of all human activities, weakening encryption, no matter the technique used, would weaken the economy as a whole, as well as our collective public safety.**

**It is worth repeating that no technique of systemic weakening of encryption could only targets criminal activities: every citizen could also be a potential target. There is no encryption-weakening technique which would only benefit to "well-meaning actors". If a backdoor is created for State activities (police, justice, intelligence services…), any other actor (other States, criminal organisations, hackers...) could potentially use it as well.**

**Is encryption used by criminals? Yes, because of their inner illegal nature, criminals try to hide their activities. But encryption is also used on a daily basis by every citizen, for almost every digital activity. Criminals can plan their activities in a closed car. Nobody would even think about banning cars, or systematically put a wire inside recording information directly accessible by State authorities.**

**However, this is the logic defended by those in favour of the criminalization or weakening of encryption. In the same way, technical capabilities for recording places (such as a car) where criminal activities may occur exists, and should be regulated by law, the technical and legal frameworks surrounding State capabilities for interception and decryption have been largely expanded in the last years, giving State agencies many opportunities to gather evidence against suspected criminal organisations.**

**Benefits provided by further weakening of encryption to fight criminality seem very low, if not uncertain. What is certain though, are the devastating consequences for citizens' rights and liberties, for the country's economy and safety, and for society as a whole.**

# 1. Encryption: a tool to protect freedoms

Protecting privacy is both a collective and an individual responsibility. Far from the usual "nothing to hide" argument that individualizes citizens in order to remove their relationships with others, privacy refers first and foremost to a concept of trust that is necessary for living in a society. Without this basic trust, the very concept of society loses its meaning. If we do not trust the safety of our communications, we cannot express ourselves or get informed without feeling monitored. Protecting our practices on the Internet has therefore an essential impact on freedom of speech, freedom of information and freedom of opinion.
It is not a choice between freedom and safety as if they were two polar opposites, but rather to accept that both are deeply related.

Yes, we all have something to hide: our communications, our browsing and our data! They must be protected.

Encryption protects our data and exchanges from prying eyes, whether they belong to malicious users, authoritarian governments, etc. That is why encryption is a necessary and essential tool for everyone. From protecting journalists' sources, medical records or legal cases to securing banking and commercial transactions (and therefore restoring "confidence in the digital economy," as in the eponymous French law: "Loi pour la confiance dans l'économie numérique"[1]), and including protecting citizens' privacy, encrypting our communication and data is a necessity.
A postcard without an envelope can be read by every single person that handles it. Likewise, an unencrypted communication sent through the Internet can be read by anyone. Encrypting communications is necessary to make sure that a message can only be read by its intended recipient. In our daily use of the Internet, using a "HTTPS" (therefore encrypted) connection is the reason why credit card transactions can be safely performed, preventing anyone with a network connection to seize your banking details.

## A global framework

In this respect, international law underline a duty of protection against any arbitrary or illegal interference in people's private lives[2]. This fundamental right does not change in the digital age. On the contrary: in 2014, the United Nations General Assembly called upon all States to "respect and protect the right to privacy, including in the context of digital communication"[3].
The United Nations Special Rapporteur on freedom of opinion and expression reminded in 2015 that restrictions imposed on encryption have broad, deleterious effects on the ability of all individuals to exercise freely their rights to privacy and freedom of opinion and expression. They must therefore be provided by law and necessary and proportionate to achieve one of a handful of legitimate objectives.
The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism concludes that "States should be transparent about the nature and extent of their Internet penetration, its methodology and its justification"[4].

[1] Law n°2004-575, 21 June 2004 « pour la confiance dans l'économie numérique ».
[2] Art. 17 of the International Covenant on Civil and Political Rights.
[3] Resolution by the General Assembly of the United Nations, 18 December 2013, n°68/167, « The right to privacy in the digital age ».
[4] 4th Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism.

# What is encryption? How does it work?

Encryption is the process of turning a clear-text message, which anyone can read, into a cyphered message which can only be understood (decrypted) with the corresponding key. There are many encryption methods (cryptology) which offer various features and can be used by different kinds of services. To understand this better, we need to make a difference between:

## Online encryption: data in motion

— **Data flow encryption:** transiting on the Internet (secure instant messaging, TLS, HTTPS[1]…). There are two types of encryption for this:

- **Point-to-point encryption (P2PE):** it is used to encrypt data as they transit, when they are being sent on the network. Data remains available in a readable form in different places on the network (on servers) where keys and certificates are stored. In this case, someone who has or gains access (authorised or not) to one of those servers can read the message.
- **End-to-end encryption (E2EE):** this method encrypts data before it is sent on the network and decrypts it only when it has arrived at its final destination. It isn't possible to decrypt the data on the way as it transits on the network. It can only be accessed from the devices (phone, computer) of the people exchanging the data.

— **Block encryption (or block cypher):** asynchronous messaging (GPG - PGP for emails, WhatsApp, Signal...)

- Point-to-point is not an option here, because encryption is receiver-tailored. It must then be an end-to-end encryption.

## Offline encryption: data at rest

Encryption of all the stored data on a phone, a tablet, a computer or a hard disk, or part of it: it is used to prevent access to the data stored on a device to any person who doesn't have the decryption key.
The method used is symmetrical encryption (by passphrase) for data that are no longer part of an exchange, but that could be accessed by third parties if a computer, smartphone, tablet, etc. happens to be stolen or lost.

[1] HTTPS protocol: it's the combination of HTTP (HyperText Transfer Protocol) and an SSL (Secure Socket Layer) encryption layer. This allows for the viewer to assess the identity of the website it browses, using a trusted third-party authentication certificate.

# 2. On the importance of secure and full encryption

## 2.1 A method increasingly questioned by States

Despite the repeated statements in favour of encryption coming from various international institutions and agencies (UNO - Office of the United Nations High Commissioner for Human Rights, special rapporteurs, General Assembly, Human rights Council, Human rights Committee -, Council of Europe[5], ENISA[6], many banking institutions, and in France the CNIL (the national Data Protection Agency)[7], CNNum (National council on digitals)[8], ANSSI (National agency of IT security)[9], etc.) many States envision enacting laws (or have already done so) intending to limit the use and access to encryption techniques. These steps are most often advocated in the name of the fight against terrorism. These weakenings do put our safety in jeopardy.

This could be witnessed when the FBI used the pretext of failing to access data stored on the iPhone of the presumed shooter of the San Bernardino attack as an attempt to force Apple into developing a back-door giving access to the content of all similar devices. It's not far-fetched to think that, beyond this individual case, the FBI was hoping to establish a case-law precedent that would have constrained the whole software industry into providing similar means of access. While finally avoided, this conflict opened the way for similar wills to legally weaken the right to encryption. Recent declarations by Paris' Republic's Prosecutor and three of his foreign counterparts (respectively English, American and Spanish) testify of this trend[10]. France's Ministry of Interior also took a public stand in favour [11] of a European initiative questioning the right to encryption.

### Possible techniques to weaken encryption

As of today, a complete prohibition of encryption seems far-fetched. However, numerous methods have been used and are still used today to weaken or limit encryption. Weakened encryption reduces the security of information and communication systems while acknowledging a "limited efficacy" – according the French National Digital Council.

[5] "Filtering, blocking and take-down of illegal content on the Internet".
[6] ENISA, « On the free use of cryptographic tools for (self) protection of EU citizens », 20 Jan. 2016 ; ENISA and Europol, "On lawful criminal investigation that respects 21st Century data protection. Europol and ENISA Joint Statement.", 20 May 2016.
[7] CNIL "Les enjeux de 2016 (3) : quelle position de la CNIL en matière de chiffrement ?", 8 April 2016.
[8] Statement of the CNNum "Chiffrement et lutte contre le terrorisme : attention à ne pas se tromper de cible".
[9] G. Pépin, "L'ANSSI défend le chiffrement de bout-en-bout, sans portes portées", NextInpact, 3 August 2016.
[10] Leppard, Cyrus R. Vance Jr, François Molins, Adrian, and Javier Zaragoza. "When Phone Encryption Blocks Justice", The New York Times, 11 August 2015.
[11] "Bernard Cazeneuve veut « une initiative européenne » contre le chiffrement". Le Monde.fr with Reuters, 12 August 2016, sect. Pixels.

- **Unencrypted points**: in an end-to-end encryption, Internet Service Providers (ISPs) provides authorities with full access to certain "points" in the network, called “taps”, where certificates and decryption keys are available, giving access to the content of communication.

- **Backdoors**: are "secret doors", security flaws, that designers would be required to put or secretly leave in their devices or services in order to give authorities access to encrypted data through this flaw. Professionals and specialized institutions, such as ANSSI (French National Security for Information Systems Agency), all agree on the fact that "backdoors may be exploited by attackers with various profiles"[1].

- **Mandatory certification for service providers**: this system was first used at the beginning of the "Crypto Wars"[2] in the United States. It compels every company to provide an encryption solution to obtain a - sometimes expensive - licence by the State, or even to give the State the decryption keys, in order for to make this solution allowed and legal in the country in question.
  This mechanism allows the State to turn illegal services deemed too powerful or escaping its control. This method can de facto prohibit every encryption system based on free software and community development.

- **Limit to the length of encryption keys**: Encryption security relies to a great extent on the ciphering key. The longer the key, the longer the time needed to break the code, making the encryption more secure. Limiting the size of encryption keys and permitting only weak keys that can be cracked by the authorities greatly reduce security, and communications confidentiality. When such a measure was imposed in the United States in the 1990's, numerous companies lost the users' trust in their services.

- **A two-speed legislation between companies and individuals:** it is important to keep in mind that encryption is as much related to cyber-security than to privacy. Having a legislation allowing, on the first side, companies to use strong encryption if they agree to grant States access to encryption keys, and, on the other side depriving individuals of any means for strong encryption, is not something excluded. Such a law cannot be tolerated: it would deny the importance of encryption for everyone's privacy.

---

[1] ANSSI « Évolution des mesures législatives relatives à la cryptographie », 24 March 2016. The risk is obviously that the backdoor is diverted from its “lawful” uses and/or discovered and exploited by malicious people.
[2] Article « Crypto Wars », Wikipedia.en, last revision 9 March 2017.

# 2.2 Encryption weakening: neither mandatory for justice, nor convenient for digital security

A right to safe encryption, without backdoors, and available to all without discrimination is mandatory. Not only will it keep or build the users' trust in digital tools and services, but it will also ensure the respect of privacy and the protection of personal data, two fundamental rights recognised by the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the articles 7 and 8 of the Charter of Fundamental Rights of the European Union[12].

## 2.2.1 Encryption in judicial proceedings

Prosecution of the most serious penal offences by the judiciary institution can justify infringement on individual and collective freedoms, under strict supervision and subject to the respect of principles of proportionality, necessity and non-excessiveness. Investigative techniques attacking encryption, like any other intrusive police technique, have to be carefully analysed. It is thereby important to ascertain which measure and under which conditions techniques countering communications encryption can be used. To that effect, the appreciation of the mean's proportionality has to be undertaken focusing on a global grasp of its consequences: the development and legalisation of some techniques could induce some effects reaching beyond the judicial framework.

It should be mentioned beforehand the current state of the law on encryption in penal cases (in France). Concerns over encrypted communications, indeed relatively recent, is not something totally new. They stem out of facts: encryption techniques (by the mean of encrypted messaging services) are sometimes used by persons in the context of illegal activities, but not limited to cases involving terrorism. Furtiveness is inner to such acts: encrypted messaging services are only a new way to achieve stealth (e.g. switching telephone chip-cards, "code speak", use of pseudonyms...). Despite this, it seems that criminals are like your "next-door net-surfer" and using encrypted messaging services is far from being unanimously adopted. The often criticized "Telegram" app seems to be used -including in jihadists circles- more for his "social networking" aspects (group discussions) than as an encrypted messaging service. Law enforcement and intelligence facilities remain large [13].

## 2.2.2 The already quite extensive judicial possibilities to decrypt data

### Broad means of expertise…

In the light of these rare, yet real practices, France's penal procedure code already foresees far-reaching prerogatives for law enforcement and judicial authorities allowing for the “decryption of encrypted data”.

During a search, article 57-1 of the Code of Criminal Procedures ("code de procédure pénale") empowers law enforcement officers regardless of the applicable penalty to request "any person likely to either have knowledge of means in use to protect the data the search allows access to or to provide them with the information enabling access to this data". Failure to answer this request is punished by a fine.

Furthermore, there's a recently modified chapter in the Code of Criminal Procedures (by laws of 13 November 2014 and 3 June 2016) whose title is "From the obtaining of cleartext from encrypted data necessary to the ascertaining of the truth" (originally in French: "De la mise au clair des données chiffrées nécessaires à la manifestation de la vérité"). A Prosecutor of the Republic as well as an investigating judge thus may, when the "seized or obtained data [...] have been subject to transformative operations hindering access to the clear-text information they contain, or to understand them, or that these data are protected by authentication means", request a legal person to carry out

[12] Charter of fundamental rights of the European Union, 200/C 364/01, 18 Dec. 2000.
[13] C. Adaoust, “Cinq moyens d’enquêter sur Telegram, la messagerie des jihadistes“. Franceinfo, 11 August 2016 et E. Leclère “Telegram : les messages postés sur le réseau social utilisé par les djihadistes ne sont ni chiffrés ni protégés“. France Inter, 16 August 2016.

"technical operations allowing access to this information, their clear-text version, as well as, were cryptologic tools are used, the secret deciphering key, if needed".

State resources covered by national security can even be put to use for any investigation pursuant to penal offences punished by at least a two-year jail term. Investigative options are thus colossal, allowing the use of the Technical Assistance Centre (TAC) at the General Directorate of Internal Security[14]. Covered with national security classification, these operations will be - notwithstanding rare exceptions - undertaken without oversight by judiciary authorities (and defence attorneys): only the technique's end result, clear-text data, is put on the judiciary file, with no means to contest the methods used.

## … based on prior data collection …

Decryption or deciphering techniques then used can in particular rely on data held available for the Prime Minister by providers of tools of encryption (for complying businesses), pursuant to the law n°2004-575 of 21 June 2004 ("Loi pout la confiance dans l'économie numérique" (LCEN)): technical specifications and source code of software that is used. Under decree n°2007-663 of 2 May 2007, the Prime Minister can in particular request the communication of the technical specifications and source code of tools of encryption that are the object of the declaration, as well as the provision of the French Network and Information Security Agency with two copies of the tools of encryption for a term that cannot exceed six months.

The 29 January 2015 order widely defines the data the administrative authority has to be provided with, that is: a description of the cryptographic features of the tool, used protocols (IPsec, SSH, SSL/TLS, VoIP-related protocols such as SIP/RTP) and cryptographic algorithms and their maximum key sizes.

## … and an incentive to self-incrimination: aggravating circumstances related to encryption.

The opportunities given to the police to attack encryption come with increasing applicable penalties up to the double amount, regardless of the offence: an aggravating circumstance is constituted "when a tool of cryptology, as defined by article 29 of law n°2004-575 of 21 June 2004 (LCEN) has been used in the preparation or commitment of a crime or offence, or to facilitate the preparation or commitment of a crime". Article 132-79 of the penal code, which provides for this increased repression, encourages defendants to provide the judicial (and the administrative) authorities with a clear-text version of encrypted messages and secret conventions necessary for decryption, to escape aggravated penalties. This provision can hardly be reconciled with the right against self-incrimination and completes a framework allowing either attacks on encryption or the decryption by the defendants themselves.

The further development of current provisions, that aims to either simply and purely banning encryption, or to introduce backdoors enabling access to clear-text data, would constitute a dangerous measure in the light of the elements above.

## A hardly measurable judicial practice (apart from the application of the Technical Assistance Centre - TAC)

The scope of applied techniques is not known. Nevertheless, a study on the impact of the law of 13 November 2014 lists the following information: "The current amount of decryption operations could only be determined for the ones implemented by the TAC. So, for the year 2013, the TAC was referred to 31 times (8 cases related to terrorism, 4 to homicides, 5 for theft or handling of stolen goods, 3 for child pornography, 2 for fraud, 3 for illegal drugs trafficking, 1 for rape and 5 for various violations), compared to 26 in 2012. For the period from January to June 2014, referrals to the TAC amounted to 13 cases."

These numbers do not take into account referrals by magistrates to private contractors specialised in decryption. There is no register of businesses or private persons pursuing this activity.

[14] Created by the decree n°2002-1073, 7 August 2002.

Even though the number of TAC referrals is stable and quite small, constant technological evolutions lead to more material being used in the context of a single referral. Similarly, some decryption operations that used to be technically unfeasible become feasible due to the progress of this service (example: damaged SIM card).

## 2.2.3 Decryption: an investigative technique among others

The focus on encrypted communication occults the fact that judicial and law enforcement authorities have already numerous investigative techniques to gather evidence at their disposal. Concealment techniques related to organised crime and terrorism are not new, whether they make use of digital technologies or not. It is true that the delay (or sometimes the impossibility) of deciphering or decryption is a reality, but this does not prevent investigative services from obtaining information by other means.

First and foremost, the means of encrypting communication do not obscure metadata and investigatory services can make use of them to obtain information (detailed phone bills remain accessible). Interception processes can also be used, to record the conversations of predetermined targets (microphones, but also since the Law of 3 June 2016, "IMSI-Catchers"). Cyber infiltration can also allow for the integration of encrypted discussion groups and then to obtain information without the necessity to break encryption. Less technical police practices are also means to obtain information in a more traditional way.

Given the provisions in force, but also the possibility to use other investigatory means and practices, a further weakening of encryption is not desirable.

This is particularly true as, no matter the legal framework that will guide this development, it will tend to evolve beyond its limitations. It is obvious to everyone that the powers given to judiciary authorities for the prosecution of criminal offenses are immediately coveted by intelligence services - if they are not already used. This does not only concern the prevention of terrorism, but also the monitoring of individuals who could threaten the economic interests or the foreign policy of France (the range of possible actions has been enlarged by the intelligence law of July 24th, 2015, to potentially include more or less radical activist organisations). If the current Minister of the Interior claims - one must admit rather selectively - that he only wants to disable encryption for judicial cases, no one must be deceived by who the other beneficiaries of this project are: intelligence services beyond all judiciary control.

The efficiency of judicial investigations, including those concerning the most serious cases, thus cannot be founded on a systemic weakening of encryption, which poses a risk on general digital safety as well as privacy rights.

***“Weakened encryption would enable mass surveillance of loyal citizens; effectiveness, necessity and proportionality of which are not proven.”***

**“*We all understand that legislators feel the need to act in reaction to events of great public concern. My recommendation is to take their responsibility for fundamental rights and the very fabric of our democracies seriously, and not to use unjustified restriction of fundamental rights lightly, because it seems and easy and low-cost measure.”***

Extracts from a speech of Giovanni Buttarelli, European Data Protection Supervisor, for the conference « Chiffrement, sécurité et libertés ».

# Proposals of the Observatoire des libertés et du numérique

**Both technical and legal capabilities for surveillance in today’s digital age are such that the fundamental right to privacy that guarantees freedom of expression, opinion and information in a democratic society has been severely challenged for the past few years, both in France and the rest of the world.**
**In these circumstances, the capacity to encrypt one's digital communication and data is an essential condition for collective security and the proper functioning of the economy, on one hand, and for the preservation of fundamental rights and liberties on the other, as it prevents arbitrary and illegal intrusion of numerous actors, be they state actors, private companies, or criminals.**

**The “Observatoire des libertés et du numérique” calls on public and private actors in the digital sector to:**

- **abstain from all initiatives, be they technological or legal, that would weaken encryption tools;**
- **consult relevant civil society stakeholders and institutions sufficiently in advance of any project that would have consequences on encryption;**
- **guarantee all individuals access to strong encryption, an essential tool for the respect of privacy in the digital sphere;**
- **promote the importance of data and communication encryption to the public, and facilitate the use and development thereof.**