

Encryption challenges in the French and European regulatory space

November 2021



Overview

Lucien CASTEX, AFNIC: castex@afnic.fr

Encryption: a maturing debate in France and in the European Union

Use case: overview of the French legal framework

- A – very – short history
- State of play

Encryption: a maturing debate

Code \leftrightarrow Language \leftrightarrow Mystery

Back to cyphers and code breaking : Lockpicking is a matter of time

A **change of scale** with the democratisation of the Internet

→ Big data and real time analysis: the **fear of surveillance**

→ **Social acceptability** of new and emerging technologies

Encryption: a maturing debate

A growing concern for security and the loss of privacy on the Internet

From freedom of speech, to data protection and freedom of assembly → **Effective implementation of fundamental rights and freedoms**

Encryption as a key tool for security and promoting fundamental rights but also perceived as an obstacle to law enforcement

Overview of the French legal framework

- A mistrust towards encryption
 - Considered a weapon of war → diplomatic and military use
 - Drastic control
- A prior authorisation system
- Encryption key length limitation: 40-bits, 128-bits
- Cumbersome procedure and complex legal regime

En 1939, décret pris en application de l'article 1^{er} du décret du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions

Les « machines cryptographiques » sont classées aux côtés des dispositifs de visée, de conduite de tir ou de détection dans les matériels de guerre en 1^{re} catégorie comptant également les « Fusils, mousquetons, carabines de tous calibres conçus pour l'usage militaire »

Overview of the French legal framework

- increased competition and technological advancement → A gradual easing with the development of the Internet
- A need to protect electronic communication in a globalisation context
- A new chapter of the crypto wars?

Loi 10 juillet 1991 relative au secret des correspondances émises par voie de télécommunications → **Principle of the secrecy of correspondence**

A number of laws: 26 July 1996, 15 November 2001 and then 21 June 2004

Overview of the French legal framework

Article 30 of the law establishes freedom of use of encryption means in France

A declaration or an authorisation process are still required for supplying, importing and exporting cryptology equipment and services

→ The French cybersecurity agency ANSSI is in charge of evaluating requests

Law n° 2004-575 of 21 June 2004 on confidence in the digital economy.

Title III on Safety in the digital economy – Chapter 1 – Cryptology methods (articles 29 to 40)

Decree N° 2007-663, provide a list of encryption means eligibility to declaration and authorisation exceptions (Annex I and II)

Overview of the French legal framework

ANSSI is in charge of prevention, defence and awareness-raising

The OCLCTIC, the French Central Cybercrime Prevention Office is in responsible for cybercrime prevention

Law n° 2004-575 of 21 June 2004 on confidence in the digital economy

Title III on Safety in the digital economy – Chapter 1 – Cryptology methods (articles 29 to 40)

Overview of the French legal framework

Use of encryption seen as an aggravating circumstance

Article 32 GDPR on Security of processing: state of the art e.g. as appropriate pseudonymisation and encryption of personal data

Article 434-15-2 Code pénal: obligation to comply with the legal requirements associated with encryption

Lifting of confidentiality

→ Article 230-1 Code de procédure pénale

Obligation to cooperate

→ Article L. 871-1 Code de la sécurité intérieure

Overview of the French legal framework

- Case Law: French Constitutional Court's decision in 2018, n° 2018-696 QPC
- Backdoors are just another security breach
- The abuses of the few should not be blamed on everyone <-> search for balance
- Key need to build trust and protect the confidentiality of electronic communications

Merci !

Contacts :

Lucien CASTEX : castex@afnic.fr



Association Française pour le Nommage Internet en Coopération

Immeuble Stephenson, 1 rue Stephenson, 78180 Montigny-le-Bretonneux, France

Tel. +33 (0)1 39 30 83 00

www.afnic.fr | contact@afnic.fr | Twitter : @AFNIC | Facebook : facebook.com/afnic.fr