Encryption: balancing privacy and national security

SUMMARY OF THE DEBATE ORGANISED BY RENAISSANCE NUMÉRIQUE AND KASPERSKY ON 28 OCTOBER 2021

With the emergence of information systems and their networking, users of the internet and IT tools have seen their data become increasingly vulnerable as they have gained access to new services. As a result, encryption, a tool for securing information systems and protecting fundamental rights and freedoms - in particular freedom of expression and the right to privacy - has become essential for economies and societies.

However, the growing need for judicial and police investigation of cyberspace in order to fight criminal organisations is leading authorities around the world to call for the weakening of encryption. While not all uses of encryption pose the same kind of problem for public authorities when it comes to apprehending criminal activities, one that is an issue for all countries in the world is end-to-end encryption. Indeed, end-to-end encryption - i.e. the obfuscation of information so that it is only available to the legitimate sender and recipients of the message, in order to guarantee the confidentiality of communications - offers new opportunities for criminal organisations to protect themselves against police and judicial investigations.

1 With end-to-end encryption, a communication service operator whose electronic communication flows are encrypted end-to-end between two users does not have access to the encryption conventions between the two users. The operator can consequently be unaware of the encryption and decryption mechanisms of the services it offers.
At the end of April 2021, Gérald Darmanin, the French Minister of the Interior, argued that it was necessary to let the government "go in and set up security breaches" within encrypted messaging systems in order to carry out investigations. This statement mirrors those of the US, Australian, and UK Justice Departments, which in a joint statement highlighted the "significant challenges to public safety" posed by modern encryption, and urged the tech industry to implement "reasonable, technically feasible solutions" to allow authorities to access backdoors when necessary. As for Olaf Scholz's newly formed German government, it has stated, through the words of SPD digital expert Jens Zimmermann, that it wants to make the defence of end-to-end encryption a priority in order to guarantee the protection of citizens' privacy.

End-to-end encryption is therefore at the forefront of current affairs and an object of tensions. Behind this debate, the balance between data security and the protection of citizens' privacy on the one hand, and national security issues such as the fight against cybercrime or terrorism on the other, is being questioned. This issue was the subject of a round table discussion organised by think tank Renaissance Numérique and cybersecurity company Kaspersky on 28 October 2021, during which legal, Gendarmerie (a police force that is part of the French armed forces), and cybersecurity experts exchanged views. During this discussion, they took stock of encryption technologies and their future prospects, and discussed the risks of their weakening, the legal framework surrounding them, and the international cooperation challenges that they entail. This summary outlines these discussions.

**Contemporary challenges faced by encryption**

Encryption faces a threefold challenge: a technical one, due to the pace of technological change; a criminal one, due to the development of new ways of organising crime, which means rethinking police and judicial investigations; and a legal one, due to the disparity of legal frameworks between countries.

---

2 « Gérald Darmanin : face au terrorisme, "il ne faut être ni résigné ni outrancier" », France Inter, 28 April 2001: https://www.franceinter.fr/emissions/l-invite-de-8h20-le-grand-entretien/l-invite-de-8h20-le-grand-entretien-28-avril-2021
IT is regularly making significant technological leaps. One of the major technological challenges facing encryption is the emergence of quantum computing, which obeys a completely different paradigm from that of today’s computers and can perform operations that current algorithms are not “resistant” to. In other words, quantum computing could make it possible to “break” encryption systems very quickly.

Encryption consists of transforming data using an encryption algorithm and an encryption key to make it unreadable. The encryption key is used by the algorithm to encrypt and decrypt the data in question. It consists of a sequence of bits, a series of zeros and ones, and is similar to a password. The encryption algorithm, on the other hand, refers to an encryption method, a way of making the data unreadable. Both the key and the encryption algorithm are needed to decrypt the encrypted data. The stronger the encryption algorithm (“irreducibility” in mathematical terms), the longer it will take to decrypt the data – without the key – or even, the more impossible it will be. Thanks to a fundamentally different processing capacity, quantum computing could reshuffle the cards. Renaud Lifchitz, Holium’s scientific director, argues that “to maintain security and therefore trust in exchanges, we need to regularly increase the size of keys so that processing power does not threaten these keys, since it is possible with computers to carry out brute force attacks and test most or all keys in order to break the encryption of a message”. However, he adds that it is not so much the size of the keys that matters, but rather the nature of the algorithms used.

Technological developments in the information technology field mean that law enforcement agencies must constantly adapt and train themselves in new digital practices in order to keep pace with criminal networks, which develop their own ways of working as technical innovations evolve. Pierre-Yves Caniotti, head of the strategy and foresight division at the Gendarmerie Command in Cyberspace, explains: “Our investigators are constantly on the alert, keeping up with the developments in digital technologies and the modus operandi of criminals, which requires constant forward planning to adapt our operations”.

---

5 In information theory, a bit is the minimum amount of information transmitted by a message. As such, it is the basic unit of measurement of information in computing.

6 In this respect, the French National Cybersecurity Agency (ANSSI) states in a recent opinion that this transition will take time, as “while prototypes of small quantum computers already exist, building large scale re-programmable ones is still at a very upstream research stage”. “ANSSI views on the post-quantum cryptography transition”, 4 January 2022: https://www.ssi.gouv.fr/publication/anssi-views-on-the-post-quan-
tum-cryptography-transition/

7 For more information on the Gendarmerie Command in Cyberspace, see the box p. 8.
In this respect, he insists on the need to increase skills: “Law enforcement agencies are now dealing with an ever-increasing volume of data to be analysed and need investigators with fairly advanced data analysis skills”. These skills are all the more necessary in the face of the widespread use of crypto-currencies within trafficking networks, which implies succeeding in tracing these assets on the internet and which therefore requires the development of new tools in order not to be left behind.

Faced with the transformation of online crime, the need for online investigation is becoming more pressing. For Pierre-Yves Caniotti, “if encryption is a challenge for law enforcement agencies, it is to protect citizens and fight against criminal organisations that use these technologies to conceal their activities (organised procuring, internet prostitution, attacks on automated data processing systems by ransomwares, etc.).”

In order to deal with these crimes, which transcend physical borders, the police and judicial authorities are trying to put in place innovative modes of action, as well as cooperation tools.

In this context, the disparity of legal frameworks between countries is a major challenge. The juxtaposition of laws that can be radically different constrains law enforcement and legal institutions in their ability to investigate, creates uncertainties for digital operators, and carries the risk of weakening citizens’ protection. According to Rayna Stamboliyska, cybersecurity expert, “this disparity is complex for everyone to manage, because we have to make sure, for example, in the case where European citizens may have to live elsewhere, that their fundamental rights are respected while respecting the sovereign legislation of the country where they reside.” In this respect, Étienne Drouard, partner at Hogan Lovells, highlights the problem of “conflict of laws” which lies in the fact that “it is not simply a question of having a French legal framework, but of knowing how it can be applied to operators over whom we have no leverage to enforce French law”.

The risks of resorting to backdoors and weak encryption

Some authorities justify the need to weaken encryption by the need to facilitate investigative processes, which are undermined by the challenges mentioned above. However, this weakening of encryption may undermine trust in digital services and devices, and increase the development of an IT vulnerabilities market.
According to some stakeholders, weakening encryption and allowing governments to introduce security loopholes would be a serious breach of “digital trust”, as it would provide the technical means for exceptional access that makes citizens vulnerable to any attempt to break into an encryption system. As long as there are accessible loopholes, any ill-intentioned person can use them to spy, steal sensitive data, or even put someone under pressure in order to obtain a ransom. Pierre-Yves Caniotti notes that “introducing backdoors natively into an information system goes against the basic rules of cybersecurity, and is likely to damage digital trust. This is tantamount to openly challenging cybercriminals to exploit this vulnerability”.

Renaud Lifchitz adds that digital trust is fundamental for the development and democratisation of new technologies in society. According to the expert, “all social and economic relations are based on trust. If we weaken this trust, we shatter all societal relations and we shatter all e-commerce and electronic trust relations”.

Furthermore, weakening encryption would contribute to the development of an IT vulnerabilities market. Étienne Drouard insists that “if we allow a market for IT vulnerabilities to develop, we will be creating an economy accessible to the highest bidder and not to those who are right. We are not sure that we have the financial or geopolitical means to draw vulnerability offers towards us or to use them in a virtuous manner in the interests of the State and the protection of our fellow citizens”. This situation would be all the more complex, according to him, as there is a legal vagueness around the possession of IT vulnerabilities. Indeed, Article 323 of the French Penal Code states that it is a criminal offence to hold the means to transform information in an information system, i.e. to be able to decrypt it. However, the article does not specify the lawfulness or unlawfulness of the possession of such a vulnerability, which puts government departments at risk of liability for the possession and use of IT vulnerabilities.

Therefore, in order not to fall into the trap that the introduction of backdoors and the weakening of encryption could lead to, other avenues should be explored that would enable investigative needs to be met while respecting citizens’ fundamental rights and freedoms.

---

8 Penal Code, Article 323-1: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000030939438/
Is the existing legal framework sufficient to ensure the balance between privacy and national security?

There are many ways to circumvent encryption without having to weaken it in a context of investigations⁹, and France has a particularly well-developed legal framework in this respect. The main issue is therefore international cooperation on a subject that concerns the sovereignty of states.

From a technical point of view, Renaud Lifchitz emphasises that “metadata analysis is interesting. Even without knowing the nature of the messages that are exchanged between a group of people, knowing the frequency of these exchanges, the constitution of a network of people, etc. can be very interesting”¹⁰ The expert also highlights the possibility of “ex-post auditability”. Indeed, he explains that “there are systems that can be audited retrospectively, known as “re-encryption” systems, in which, during an investigation into electronic communications, it is possible to reveal the history of the communications retrospectively”. To make this possible, it would be a simple matter of “imposing standards on electronic communications providers”. On these points, Pierre-Yves Caniotti emphasised that the Gendarmerie is working “in cases specifically regulated by law and in frameworks specifically targeting organised crime, on the implementation of advanced decryption methods and specific techniques such as IT data capture as defined by the code of penal procedure”.

In this respect, the French legislative framework concerning encryption is quite developed. According to Étienne Drouard, “the issue of security and freedom around encryption is well regulated in French law. When it comes to making non-disclosure of encryption methods illegal, this prohibition has existed in French law since 2015 in Article L-871 of the Internal Security Code¹¹. Anyone who does not provide the keys necessary for public services to carry out their duties, is liable to imprisonment”. Pierre-Yves Caniotti also notes that technology is evolving at such a pace that the challenge consists in dealing with these technical developments, rather than with legal requirements.

---

⁹ For example, the (legal) possibility for the police to use malwares to infect the computers of suspects.
¹⁰ It should be noted here that this source may eventually dry up as well. In this respect, the work carried out by Signal to reduce or encrypt the metadata itself is interesting. It is possible that other messengers may be forced to follow suit. For more on Signal’s work, see: https://signal.org/blog/sealed-sender/
¹¹ Internal Security Code, Article L871-1: https://www.legifrance.gouv.fr/codes/article_lc/LEGIAR-TI000030937647/
However, the international dimension of the problem poses limitations to the application of the existing framework. A joint vision on encryption issues is hard to implement. To illustrate this difficulty, Rayna Stambo-liyska takes the example of the debate on the e-Privacy Regulation\(^\text{12}\) within the European Union (EU). Although this text, which is supposed to replace the 2002 e-Privacy Directive, should have been adopted at the same time as the General Data Protection Regulation (GDPR), i.e. in 2016, discussions have stalled. According to the expert, this inability of EU Member States to agree on certain points means that, in terms of both encryption and personal data protection, we remain, in some respects, “in the dark”. The introduction of a more homogeneous legal framework for encryption at European level is thus hampered by “different governments’ divergent practices”.

The issue is all the more complex as it is not only a matter of judicial and police affairs, but also of intelligence activities, which Étienne Drouard insists on by explaining that “like all countries, we do not have relationships of friendship, but relationships of interest. What structures the European Union are common objectives. On the subject of intelligence, no country is willing to entrust parts of its intelligence to others. That would be contrary to the principle of sovereignty. There is no federalism when it comes to intelligence”.

The question of striking a balance between national security and the right to privacy through encryption thus comes up against the complexity of geopolitics. Nevertheless, the existing framework, although it can be improved, makes it possible to avoid the temptation to weaken encryption and to preserve “digital trust”. According to Rayna Stambo-liyska, the debate on weakening encryption that has been going on for several years is outdated, and the discussion is “putting the objective of punishing the perpetrators and protecting the victims back at the heart of the matter”.

GENDARMERIE COMMAND IN CYBERSPACE

Officially created on 25 February 2021\(^\text{13}\), the Gendarmerie Command in Cyberspace (ComCyberGend) aims to bring together the actions carried out by the Gendarmerie in order to fight against cyber threats and crime in cyberspace. In particular, it integrates the Centre for Combating Digital Crime (C3N) and the National Gendarmerie Criminal Research Institute’s IT-electronic department, with the aim of bringing together its cyber forces and thus increasing its effectiveness in terms of investigation and prevention.

Source: COMCyberGEND\(^{14}\)

---

\(^{13}\) Order of 25 February 2021 on the creation of the Gendarmerie Command in Cyberspace: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043261338


---

Author

Arthur Druel-Hodak, Project assistant, Renaissance Numérique

Proofreading

Jennyfer Chrétien, General Manager, Renaissance Numérique
Arnaud Dechoux, Public Affairs Manager Europe, Kaspersky
Jessica Galissaire, Studies Manager, Renaissance Numérique
Noémie Minster, Corporate Communications Manager, Kaspersky

Renaissance Numérique and Kaspersky would like to warmly thank the speakers and participants in this debate, which was held as part of the European Cybersecurity Month.