For a More Effective Fight against Cybercrime

Myriam Quéméner

Advocate General at the Court of Appeal of Paris; Doctor of Law

Abstract

Cybercrime is, by its very nature, an organized and international form of crime that does away with borders by means of digital networks. Cyberspace offers a limitless digital field, tools that are now easily accessible, and a growth in the number of potential victims, which has the effect of increasing the harmfulness of this criminal phenomenon. Moreover, there are growing challenges in terms of information systems security, on the one hand because of the exacerbation of cyberthreats, and on the other because of the ever-increasing use of systems that host often-sensitive personal data. Cybersecurity is also one of the major challenges of the twenty-first century. It is already on the European legislator's agenda, and the fight against cybercrime is now a central priority

Keywords: cybercrime, cyberthreat, law

Para una lucha más efectiva contra el cibercrimen

Resumen

El ciber crimen, por naturaleza propia, es una forma de crimen organizado internacional que desvanece las fronteras a través de redes digitales. El ciber espacio ofrece un campo digital ilimitado, herramientas que son ahora fácilmente accesibles, y un creciente número de potenciales víctimas, lo cual tiene el efecto de incrementar el daño potencial de este fenómeno criminal. Adicionalmente, hay más y más desafíos en materia de la seguridad de sistemas de información, por un lado debido a la exacerbación de amenazas cibernéticas, y por otro lado por el creciente uso de sistemas que alojan datos personales sensibles. La ciber seguridad también es uno de los mayores retos del siglo XXI. Ya está en la agenda de los legisladores europeos, y la lucha contra en ciber crimen ya es una prioridad central.

Palabras clave: ciber crimen, ciber amenaza, ley

 doi: 10.18278/ijc.7.1.3

更有效地打击网络犯罪

摘要

本质上，网络犯罪是一种通过数字网络摆脱边界的有组织国际犯罪形式。网络空间提供了一个无限数字领域和容易获取的工具，造成了潜在受害者数量的增加，这产生了增加犯罪现象的危害性的效果。此外，在信息系统安全方面存在越来越多的挑战，一方面是因为网络威胁的加剧，另一方面是因为对“存储经常具有敏感性的个人数据”的系统的使用不断增加。网络安全还是21世纪的重大挑战之一。欧洲立法者已

将其提上议程，并且打击网络犯罪是一个首要的优先事项。

关键词：网络犯罪，网络威胁，法律

Cybercrime[1] is, by its very nature, an organized and international form of crime that does away with borders by means of digital networks. Cyberspace offers a limitless digital field, tools that are now easily accessible, and a growth in the number of potential victims, which has the effect of increasing the harmfulness of this criminal phenomenon. Moreover, there are growing challenges in terms of information systems security, on the one hand because of the exacerbation of cyberthreats,[2] and on the other because of the ever-increasing use of systems that host often-sensitive personal data. Cybersecurity is also one of the major challenges of the twenty-first century. It is already on the European legislator's agenda, and the fight against cybercrime[3] is now a central priority for governments.

Sizeable Cyberchallenges

Besides problems arising from the transnational nature of investigations and prosecutions, criminal law standards sometimes struggle to adapt to cybercrime because constantly evolving technologies create new modes of operation for criminals.

1 Myriam Quéméner and Yves Charpenel, *Cybercriminalité. Droit pénal appliqué* (Paris: Economica, “Pratique du droit” series, 2010), 7.

2 Ministry of the Interior, État de la menace liée au numérique en 2018 (Paris: Ministry of the Interior, 2018), www.interieur.gouv.fr.

3 William Roumier, “Justice pénale dans le cyberespace,” *Droit pénal* 7-8 (July 2017): alert 48.

Digital data have become the focus of a real power struggle between states that want control over data circulating within their territory and between private companies that provide the networks through which data are channeled. The interest generated in this truly immaterial wealth reflects the transformations that geopolitics has undergone in the digital age: a questioning of physical national borders, an affirmation of private and nonstate actors, a "digitization" of conflicts and claims regarding sovereignty in cyberspace, and cyberattacks.

Controlling data requires knowledge of the means and conditions of their production, their transmission channels, and how and where they are stored.[4] Data create value and power, and they are "the link between physical and digital spaces." Data and their control are reconfiguring the balance of power at the strategic and economic levels, and they are giving rise to new representations of sovereignty.

We are also seeing the development of "cyberhavens": states with weak or nonexistent legislation. Moreover, traditional legal tools are inadequate because they take too long to implement,[5] given that electronic evidence is ephemeral; this makes it more difficult to identify cybercriminals. And then there are attacks against automated data-processing systems, such as distributed denial-of-service (DDos) attacks, including instances of hacking, particularly those launched from abroad.

The international dimension of cybercrime[6] entails a harmonization of national laws, or at least the facilitation of cooperation at the European and international levels in order to strengthen the means of fighting this phenomenon. Criminal proceedings may face obstacles or be slowed down by the international nature of this type of crime.

When service providers are not established in the European Union, a request for international mutual legal assistance in criminal matters should be made. The implementation of these procedures can be further complicated if the service provider's data are located in multiple countries. This can then lead to other issues relating to the location of the data and the determination of the jurisdictions territorially competent to access them.

There are major challenges here, and one cannot overlook their geopolitical and strategic aspects, with the emergence of extraterritorial legislation that could harm Europe, such as the Clarifying Lawful Overseas Use of Data Act, or CLOUD Act. Although the CLOUD Act,[7] adopted by the United States Congress on March

4 Myriam Quéméner, "Le droit face à la disruption numérique," *LGDJ* (2018).

5 Ten months on average for requests for international mutual legal assistance in criminal matters (CRI or MLAT—Mutual Legal Assistant Treaty—in the case of the United States), with a maximum response time for a European Investigation Order set at 120 days.

6 "Cybersécurité, cybercriminalité: quelles réponses stratégiques et juridiques?," special report, *Dalloz IP/IT 3* (March 2018): 158.

7 Garance Mathias and Aline Alfer, "Conséquences du Cloud Act pour les européens?" *Expertises*

23, 2018, provides that data can only be transferred in certain specific cases (prosecution and prevention of serious offences; precise identification of the information requested and the individual in question), it is necessary to remain vigilant.

Therefore, overlaying geopolitical competition between the most powerful countries is a confrontation taking place in cyberspace, within a curious mixture of defense of national sovereignty and a quest for the widest extraterritoriality. One should not overlook the threat that an oligopoly of companies will capture data and use their dominant position to obstruct new players. Apart from these aspects, there are also "creeping" extraterritorialities related to digital technologies. The most dramatic example here is the United States.

France is reacting to this phenomenon by bringing in legislation that on the one hand protects its information systems via the Directive on the Security of Network and Information Systems (NIS), which was transposed into French law in February 2018, and that on the other hand protects the country's personal data via the General Data Protection Regulation (GDPR), which has an extraterritorial dimension since it imposes on all companies measures to protect personal data. European legislation falls within a sovereignty-based approach, starting with that of each member state in relation to its personal data.

I. Progress and Perspectives

The European Union has mechanisms for police and judicial cooperation that facilitate the fight against vulnerabilities. The European Union detected the issues surrounding cybercrime very early on. For this reason, in January 2013, it set up the European Cybercrime Centre within Europol (European Police Office). The main objective of this center, which is also known as EC3, is therefore to fight cybercrime.

In terms of legislation, it should first be recalled that the Council of Europe's so-called Budapest Convention on cybercrime, which was signed on November 23, 2001 and ratified in France on May 19, 2005, remains the binding international instrument of reference in the fight against cybercrime.

The drafting of a second additional protocol to this convention[8] has been under way since September 2017. The protocol envisages measures that aim to simplify judicial cooperation between the fifty-six countries that are parties to the convention and to facilitate direct cooperation with internet service providers from other member countries. Particular areas under study are greater opportunities for cross-border access to data by investigative services, a simplified framework for mutual legal assistance requests concerning subscriber data, and a formalization of emergency procedures.

436 (2018).

8 Pierre Berthelet, "Aperçus de la lutte contre la cybercriminalité dans l'Union européenne," *Revue de science criminelle et de droit pénal comparé* 1 (2018): 59.

These works are consistent with those carried out in the European Union framework, and this project is expected to conclude in 2019.

Within the United Nations General Assembly, in 2011 the Commission on Crime Prevention and Criminal Justice was tasked with creating an intergovernmental expert group (IEG) devoted to drafting a comprehensive study on the phenomenon of cybercrime. In 2013, the group submitted its report, which revealed a division within the international community over whether or not it was necessary to supplement the existing legal framework.

Debates highlighted significant differences of opinion over the international legal instruments to be used in the fight against cybercrime. A majority of states, including France, were reluctant about a new international legal text, declaring themselves in favor of using the Budapest Convention as the legal basis for the fight against cybercrime.

One solution in my mind is to develop a genuine and coherent cybersecurity law,[9] rather than one that is scattered across multiple codes and texts.

The European Investigation Order (EIO)

Directive 2014/41/EU of the European Parliament and of the Council of April 3, 2014, regarding the European Investigation Order in criminal matters[10] endeavors to unify European law on the obtaining of evidence. The European Investigation Order replaces all of these procedures and is thus part of an essential simplification of procedures.[11] It is a significant advance in the field of judicial cooperation because it provides an instrument that is more consistent with the legal ambitions of the EU and the crime-related challenges that it faces. This tool should prove to be essential in effectively fighting crime in Europe, as the transnational dimension of crime continues to grow. It must also be an opportunity to promote a more systematic handling of the various facets of crime, and in its particular economic and financial aspects.

The New Directive on Combating Fraud and Counterfeiting of Non-Cash Means of Payment

The European Commission intends to obtain additional means of responding to cyberattacks. According to the Commission, the current legal framework for combating fraud and counterfeiting of non-cash means of payment (Framework Decision 2001/413/JHA, May 28, 2001) is no longer in sync with today's technological

9 Thibault Douville, "L'émergence d'un droit commun de la cyber-sécurité," *Recueil Dalloz* 39 (2017): 2255-65.

10 https://eur-lex.europa.eu.

11 Thomas Cassuto, "La directive concernant la décision d'enquête européenne en matière pénale," *AJ pénal* (2014): 338.

developments and challenges, and so it is proposing to adopt effective repressive and "cyberdeterrence" criminal law measures through a new directive.

Furthermore, the proposed directive[12] will broaden the scope of cybercrime offenses through the inclusion of transactions carried out using virtual currencies. It will also introduce common rules on sentences, which will carry a term of imprisonment ranging from a minimum of two years to a maximum of five years. It will also clarify the scope of member states' jurisdictional competence in relation to these offenses and will guarantee the rights of victims of cybercrime.

Finally, by strengthening cooperation in criminal matters at the European level, the directive will aim to facilitate cross-border access to electronic evidence. To this end, in October 2018 the Commission will present its conclusions on the role of encryption in criminal investigations.

The Draft Directive and Regulation of E-evidence

On April 17, 2018, the European Commission presented a draft directive and a draft regulation on access to electronic evidence in criminal matters. These will need to be adopted by the Council of the European Union and the European Parliament. Today, law-enforcement authorities are often dependent on the goodwill of service providers to hand over the evidence that they need. The aim is to provide legal certainty to businesses and service providers by applying the same rules to order the provision of electronic evidence.

These texts include plans to establish a European Production Order. This will allow a judicial authority in a member state to directly request electronic evidence (such as emails, text messages, or messages in apps) from a service provider that offers services in the EU and that is established or represented in another member state, regardless of where the data is stored. The service provider will be required to respond within ten days, and within six hours in an emergency (as opposed to 120 days for the existing European Investigation Order or ten months for a mutual legal assistance procedure).

Preventing the deletion of data through a European Preservation Order will allow a judicial authority of a member state to oblige a service provider offering services in the EU and established or represented in another member state to retain certain data so that the authority can request this information later through mutual legal assistance or through a European Investigation Order or a European Production Order.

The new rules ensure strong protection of fundamental rights, such as the intervention of judicial authorities and additional requirements on obtaining certain categories of data. They also include guarantees regarding the right to the pro-

12 *Dalloz actualité*, September 25, 2017, European Commission Communiqué, September 19, 2017, IP/17/3193.

tection of personal data. Service providers and persons whose data are requested will enjoy several safeguards, including scope for the service provider to request a review if, for example, the order constitutes a clear violation of the Charter of Fundamental Rights of the European Union.

Service providers will be obliged to appoint a legal representative in the EU. So that all service providers that offer their services in the EU are subject to the same obligations, even if their headquarters are located in a third country, the new rules require them to appoint a legal representative in the EU to receive, comply with, and execute decisions and orders issued by the member states' competent authorities for the purposes of gathering evidence in criminal matters.

Institutional Actors' Competence

Judicial police officers are becoming specialized, as are customs agents, and judges will gradually have to follow this path too. The creation in September 2014 of **Section F1 of the Paris prosecutor's office**, which specializes in cybercrime, and the recent **concurrent domestic jurisdiction**[13] **of the Paris courts in relation to computer hacking** (attacks on automated data-processing systems) facilitate coordination in the handling of cybercrime.[14] It therefore appears that concurrent competence over attacks on automated data-processing systems can be understood based on several objective criteria, some of which are cumulative: the plurality of perpetrators or victims; the technicality of the means employed or the operating methods adopted (the "Mirai" case; "black box" attacks targeting ATMs; cybercriminal forums on a darknet, and so on); the national or transnational dimension of the facts or infrastructure (requests for international mutual legal assistance in criminal matters made to China and Russia are frequent in this area; coordination required in connection with Europol, Eurojust, and Interpol); the nature of the victims of the cyberattack (automated data-processing systems implemented by a state, but also by operators of vital importance, or computer systems linked to high-profile individuals). The competent investigation service is frequently the French General Directorate for Internal Security (DGSI), sometimes with the benefit of technical expertise from the National Cybersecurity Agency (ANSSI).

However, staff levels are still insufficient, and training for judges and prosecutors in charge of these "cyberproceedings" should be mandatory.

Moreover, it should not be forgotten that, in 2020, the European Public Prosecutor's Office[15] will be a reality, paving the way for enhanced cooperation, under which twenty states (soon to be twenty-one, with the Netherlands joining the agreement this summer) have committed to concede some of their sovereignty

13 Law of June 3, 2016.

14 For example, on the handling of ransomware (DACG report of May 10, 2017, no. 2017/0058/MI2C).

15 "Parquet européen: c'est parti!," special report, *AJ pénal* (2018): 275.

in order to more effectively combat attacks against the European Union's financial interests. But Regulation no. 2017/1939 of October 12, 2017 and the "PFI" Directive (no. 2017/1371 of July 5) far from resolve all difficulties. The evolution of the European Public Prosecutor's Office will be watched not only by member states that are not yet part of the enhanced cooperation regime but also by international observers, since it is a very innovative mechanism for fighting the massive levels of fraud that deprive states of billions of euros in tax revenue each year. In the medium term, one cannot rule out an extension of competence to other forms of crime linked to the digital world. But the institution's success or failure will largely depend on the content of the transposition texts of the directive, which must be adopted before July 6, 2019.

Public/Private Cooperation

To the extent that cyberattacks cannot be proved without turning to the private sector, which often holds key evidentiary elements, the fight against this scourge entails strengthening interactions with both internet giants and operators. For example, an agreement on sharing information on cyberthreats has recently been concluded between Orange and Europol. It entails an exchange of information on network statuses and threats, as well as on cybercrime trends. The French operator has agreed to supply Europol with indicators of fraud, spam, and cyberattacks on mobiles and banking services that it may see on its networks. Through this activity, Orange, which has a presence as a telecommunications operator in seven European countries, hopes to offer its customers and users across the world a "safer internet." Their combined efforts aim to create a safer cyberspace for all actors in the European Union: citizens, governments, and businesses.

One could mention the recent extraordinary "black hand" operation, which was led by customs agents and dismantled one of the largest active illegal platforms in France on the "dark web."

In provisional conclusion, areas for improvement in the fight against cyberthreats require a speeding up of the processes of drafting legal standards in the face of rapidly evolving digital capabilities. Avenues for action must focus, on the one hand, on procedures for access to electronic evidence, which should be standardized as part of a goal of achieving legal certainty, and, on the other hand, on digital identity in order to ascertain the perpetrators of these harmful actions.

CYBERCRIME – CYBERTHREATS – LAW

Cybercrime[16] is, by its very nature, an organized and international form of crime that does away with borders by means of digital networks. Cyberspace offers a

16 Myriam Quéméner and Yves Charpenel, *Cybercriminalité. Droit pénal appliqué* (Paris: Economica, "Pratique du droit" series, 2010), 7.

limitless digital field, tools that are now easily accessible, and a growth in the number of potential victims, which has the effect of increasing the harmfulness of this criminal phenomenon. Moreover, there are growing challenges in terms of information systems security, on the one hand because of the exacerbation of cyberthreats,[17] and on the other because of the ever-increasing use of systems that host often-sensitive personal data. Cybersecurity is also one of the major challenges of the twenty-first century. It is already on the European legislator's agenda, and the fight against cybercrime[18] is now a central priority for governments.

17 Ministry of the Interior, État de la menace liée au numérique en 2018 (Paris: Ministry of the Interior, 2018), www.interieur.gouv.fr.

18 William Roumier, "Justice pénale dans le cyberespace," *Droit pénal* 7-8 (July 2017): alert 48.