REGULATING CYBERSECURITY

BY
BÉNÉDICTE SCHMITT

Bénédicte Schmitt is an experienced senior manager with a demonstrated history of working in and with national and international organizations. Graduated from Sciences-Po Lille (France), the Jean Monnet Centre of Excellence in Turku (Finland), the Universities of Paris 1 and 2 (France), and the College of Europe in Bruges (Belgium), she is skilled in European and international laws and policies, with a specific focus on cyber security. In the past 6 years, she has been representing the French government across a wide range of international partners, addressing the future of cybersecurity regulation, policies, and products.

REGULATING CYBERSECURITY

By Bénédicte Schmitt

With the increasing dependence of our societies on computer systems and the Internet, and the explosion of so-called "smart" and connected devices, cybersecurity is taking on unprecedented importance. Not so long ago, cybersecurity was a technical domain reserved for IT experts in order to protect digital infrastructures. Today, it has become an unavoidable political and social subject that has been invited to the discussion table, whether it be for international organizations, States, major global companies, local entrepreneurial micro-structures, or even individuals. This raises the question of cybersecurity regulation. What are the different initiatives that currently exist? Is it possible to regulate cybersecurity at a global scale with a one-size-fits-all strategy?

With the increasing dependence of our societies on computer systems and the Internet, and the explosion of so-called "smart" and connected devices,[2] cybersecurity is taking on unprecedented importance.

Not so long ago, cybersecurity was a technical domain reserved for IT experts in order to protect digital infrastructures. Today, it has become an unavoidable political and social subject that has been invited to the discussion table, whether it be for international organizations, States, major global companies, local entrepreneurial micro-structures, or even individuals.

This raises the question of cybersecurity regulation. What are the different initiatives that currently exist? Is it possible to regulate cybersecurity at a global scale with a one-size-fits-all strategy?

Cybersecurity regulation refers to the laws, policies, and standards that are put in place to protect against cyber threats and to ensure the secure operation of computer systems and networks.

One of the main goals of cybersecurity regulation is to establish a set of best practices and requirements for organizations or States to follow in order to protect their systems and data from cyber threats. This can include things like requiring the use of strong passwords, implementing security measures such as firewalls and antivirus software, and regularly updating software to fix vulnerabilities.

Considering the globalization of cyber threats, States were quick to recognize the need for a common international response. However, this response is hampered by the reluctance of States to share certain information that could affect their national security and, above all, by fundamental differences in the way States view their cybersecurity and consider the measures to be put in place to reinforce it. Consequently, as things stand, there is no binding international law on cybersecurity.

International cooperation initiatives have however been observed since the beginning of the 1990s, particularly at the level of the Organization for Economic Cooperation and Development ("OECD").

Based on the premise of the increasing use of computers and the international nature of information systems, the OECD member countries felt the need to raise awareness of the risks threatening information systems and the means to protect themselves against these risks. Thus, the first Guidelines for the Security of Information Systems were issued in 1992.[3]

These guidelines, which were replaced and updated in 2022,[4] are not legally binding. They are recommendations that the OECD members are encouraged to follow in order to facilitate international cooperation and to work collectively to strengthen the security of information systems. Subsequently, other recommendations[5] have been developed by the OECD to strengthen "digital security," a term that the OECD favors over "cybersecurity"[6] at the international level.

In 2001, another international organization, the Council of Europe, initiated the first international cyber security cooperation treaty. Known as the Budapest Convention,[7] this treaty is designed to address the challenges posed by cybercrime and to provide a framework for international cooperation in investigating and prosecuting cybercrimes.

One of the main goals of cybersecurity regulation is to establish a set of best practices and requirements for organizations or States to follow in order to protect their systems and data from cyber threats

The Budapest Convention is the first international treaty on cybercrime and is considered to be the benchmark for international cooperation in this area. It establishes standards for criminalizing various cyber activities, such as hacking and the distribution of malicious software. The Convention

2 The number of Internet of Things ("IoT") devices worldwide is forecast to almost triple from 9.7 billion in 2020 to more than 29 billion IoT devices in 2030. https://www.statista.com.

3 C(92)188/FINAL.

4 https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0312.

5 For example, Guidelines on Cryptography Policy (1997), Recommendation on Digital Security of Critical Activities (2019), Recommendation on National Digital Security Strategies (2022).

6 According to OECD, "Digital security refers to the economic and social aspects of cybersecurity, as opposed to purely technical aspects and those related to criminal law enforcement or national and international security." https://www.oecd.org/digital/ieconomy/digital-security/.

7 Convention on cybercrime (STE n° 185).

also provides a framework for international cooperation in investigating and prosecuting cybercrimes, including provisions for mutual legal assistance, extradition, and the collection and exchange of evidence.

In addition to establishing standards for criminalizing cybercrimes, the Budapest Convention also includes provisions on the protection of personal data and the promotion of international cooperation in the field of cybersecurity.

Overall, the Budapest Convention is an important international treaty, which has been now signed by 68 countries,[8] that helps to combat cybercrime and promotes international cooperation in addressing these challenges.

While the first regulatory initiatives at the international level remain subject to the goodwill of States, the European Union ("EU") has gradually set itself apart by making cybersecurity measures applicable throughout the Union mandatory.

Since its creation in the 1950s, the number of subjects regulated by the EU, whether in exclusive or shared competences, has continued to grow, and cybersecurity is no exception.

Since the beginning of the year 2000, the EU has initiated proposals and action plans to strengthen the security of digital networks on the EU territory.[9] But considering the strong disparities between Member States in terms of available resources, the lack of coordination between States in the event of incidents, and the need to better prepare and involve the private sector, the European Commission decided to create a dedicated technical agency. The European Union Agency for Network and Information Security ("ENISA") was therefore created in 2004[10] to help the Union reach a higher level of cybersecurity.

The decision to create a decentralized technical agency, with its own legal personality distinct from the European institutions, enables it to position itself on two levels. Not only does ENISA support the development of European public policies by proposing technical norms and standards, but it is also meant to act as a privileged interface with the Member States by promoting cross-border cooperation between Member States, and by developing assistance and consulting capabilities.

In March 2010, the European Commission launched the "Europe 2020" strategy,[11] whose objective is to relaunch and prepare the economic growth of the EU by adapting its policies to future challenges. With no surprise, digital issues are presented as one of the main future challenges, hence the publication two months later of a digital strategy for Europe, also known as "Digital Agenda for Europe".[12]

A further notable step was taken in 2013 with the presentation of the first cyber security strategy for the European Union.[13] While recognizing that the primary responsibility for addressing security issues in cyberspace rests with the Member States, the strategy identifies five priority areas,[14] and announces the implementation of binding measures for Member States to strengthen the overall level of cybersecurity on the territory of the Union.

> ***"The decision to create a decentralized technical agency, with its own legal personality distinct from the European institutions, enables it to position itself on two levels***

Indeed, on the same day as this strategy, a proposal for a directive[15] was published in order to guarantee a high common level of security for information systems. This direc-

8 https://www.coe.int/en/web/cybercrime/parties-observers.

9 The European Commission adopted in 2001 a Communication on "Network and Information Security: Proposal for a European Policy Approach" (COM(2001) 298) and in 2006 "A Strategy for a Secure Information Society" (COM(2006) 251). Since 2009, the Commission has also adopted an action plan and a communication on the protection of critical information infrastructures (COM(2009) 149 approved by Council Resolution 2009/C 321/01, and COM(2011) 163 approved by Council conclusions 10299/11].

10 Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.

11 COM(2010) 2020 final.

12 COM(2010)245 final.

13 JOIN(2013) 1 final, Cybersecurity Strategy of the European Union. An Open, Safe, and Secure Cyberspace.

14 Ensuring "cyber resilience," drastically reducing cybercrime, developing a cyber defense policy and capabilities in the framework of the EU's military missions, developing a network of cybersecurity technological and industrial resources for the EU, defining an international cybersecurity strategy defending the EU's values.

15 COM(2013) 48 final.

tive, which was officially launched in July 2016 under the name "NIS Directive,"[16] is a unique regulatory act in that it imposes major mandatory measures to be taken by the Member States.

As an example, the directive requires all EU Member States to set up and implement national cybersecurity authorities, national cyber incident response teams ("CSIRTs") and national cybersecurity strategies. It also obliges Member States to strengthen security measures and infrastructure resilience in sectors deemed critical, such as energy, transport, public administration, economy, as well as to impose the reporting of incidents and/or attacks, and to strengthen cooperation procedures between Member States.

The national transpositions have enabled the appearance of new regulatory tools in all Member States, constituting, at the European level, an undeniable advance in the level of digital security. The NIS directive has also been an effective vector for increasing the level of security around the actors essential to the functioning of the economy and society of the EU Member States.

All in all, the NIS Directive is the first binding horizontal internal market instrument and can be regarded as the first EU cybersecurity law.

A new version of the NIS Directive, better known as the "NIS 2 Directive,"[17] has been recently published in December 2022 to enlarge the scope of application to new sectors,[18] which will considerably increase the number of regulated entities. It also strengthens and streamlines security and reporting requirements for companies by imposing a risk management approach and by providing a minimum list of basic security elements that must be applied such as risk analysis.

Furthermore, NIS 2 addresses security of supply chains and supplier relationships by requiring individual companies to address cybersecurity risks in the supply chains and supplier relationships. In addition, it introduces more stringent supervisory measures for national authorities, and stricter enforcement requirements. Finally, it also aims at harmonizing sanctions regimes across Member States. This Directive must be transposed within all EU Member States by October 2024.

However, due to the growing number of security incidents and attacks relating to information and IT systems and the digitization of our societies to all domains, including critical ones such as healthcare and energy, it is impossible to solely rely on horizontal binding rules even at a regional level such as the EU territory. As cybersecurity is highly transversal, the need for vertical measures has become obvious.

Since the 1990s, technical standards have tended to develop as a type of cyber regulation at the international level. Cybersecurity standards are statements that describe what must be achieved in terms of security outcomes in order to fulfil an enterprise's stated security objectives.

The aim of standards is twofold. First, they guarantee to users the security of digital tools and devices, as well as communication networks. But they also facilitate trade between countries all over the world by bringing interoperability, harmonization of terminology, performance checking, security evaluation, supply chain integrity and security.

Standardization activities take place in international, national, and industry-based fora.

At the international level, one cannot but mention the ISO/IEC 27000-series, also known as the "ISMS Family of Standards" or "ISO27K," which are jointly developed and published by the International Organization for Standardization ("ISO")[19] and the International Electrotechnical Commission ("IEC").[20]

> ***Since the 1990s, technical standards have tended to develop as a type of cyber regulation at the international level***

The ISO/IEC 27000 family is a series consisting of various information security standards that set out guidelines and requirements for implementing an Information Security Management System ("ISMS") with the aim of managing

16 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

17 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union.

18 Public administration, space sector, digital service providers, wastewater and waste management systems, postal services, food, chemical and pharmaceutical manufacturers.

19 https://en.wikipedia.org/wiki/International_Organization_for_Standardization.

20 https://en.wikipedia.org/wiki/International_Electrotechnical_Commission.

information security within an organization.[21] Those standards are used all over the world and are considered to be the first reference for cybersecurity standardization.

At the European level, three European Standardization Organizations, the European Committee for Standardization ("CEN"), the European Electrotechnical Committee for Standardization ("CENELEC") and the European Telecommunications Standards Institute ("ETSI"), have been officially recognized by the European Union and by the European Free Trade Association ("EFTA") as being responsible for developing and defining voluntary European standards. These standards set out specifications and procedures in relation to a wide range of materials, processes, products, and services.

These European organizations all play an active role in developing technical standards to raise the level of cyber security. They also work very closely, together with ENISA, so as to avoid overlapping contradictions or incompatibilities between standards.

ENISA's role in standards has been strengthened since the Cybersecurity Act[22] came into force in 2019. This Regulation aims to create a robust cybersecurity legislative framework for the European Union and to standardize standards and processes for the European space.

The Cybersecurity Act is divided into two parts. The first part formalizes a permanent and enhanced mandate for ENISA. The second part introduces a European cybersecurity certification framework for information and communication technology products, services, and processes.

Besides, the European Commission has recently published a Cyber Resilience Act,[23] which aims at setting common cybersecurity standards for connected devices and services.

National standardization bodies are also producing high value standards, like for example the U.S. National Institute of Standards and Technology ("NIST") which develops standards and guidance to help organizations assess risk. NIST for instance released in 2014 a Framework for Improving Critical Infrastructure Cybersecurity and in 2018 a Cybersecurity Framework which are widely applied.

Although many enterprises choose to adopt a generic industry cybersecurity standards framework, it may not address all the enterprise's regulatory and business obligations. This is because generic standards do not consider industry-specific or regional requirements. Therefore, in addition to regulatory requirements, a number of industry-specific standards has emerged. For example, the Payment Card Industry Data Security Standard ("PCI DSS") is a set of security standards that apply to organizations that handle credit card transactions. Society for Worldwide Interbank Financial Telecommunication ("SWIFT") has initiated a Customer Security Program ("CSP") helps financial institutions ensure their defenses against cyberattacks are up to date and effective, to protect the integrity of the wider financial network.

In conclusion, given the explosion in the number of cyberattacks, the intensity of which is increasing year after year, cybersecurity regulation appears to be one of the necessary and indispensable response levers to help governments and companies face cyber threats.

An organization can thus rely on families of international standards, recommendations and guidelines developed by international political or sectoral organizations, but also national guides published by national agencies in charge of cybersecurity, or even security policies in use at the national level that may result from a mandatory transposition of an EU document.

An organization therefore has a multitude of cyber regulatory tools at its disposal to help it deal with cyber risks, depending on several parameters such as its size, its sector of activity, its criticality, its geographical location, and its area of activity.

In this sense, cyber regulation cannot respond to a "one-size-fits-all" logic and must instead be constantly adapted to meet the technical, political, social, and economic challenges of cyber threats.

However, increasing prescriptiveness among cybersecurity regulation may lead to overwhelming and overlapping documents that do not align. The continuous increase of regulations can make it difficult for organizations to comply with all the rules, standards, laws, guidelines, etc. It can also become very confusing, and, in the end, have counter effects by impeding interoperability and innovation.

All in all, as cybersecurity regulation is unavoidable the only way to avoid those negative aspects is to encourage international collaboration between States, but also between the public and the private sectors.

21 https://www.globalsuitesolutions.com/information-security-iso-27001/.

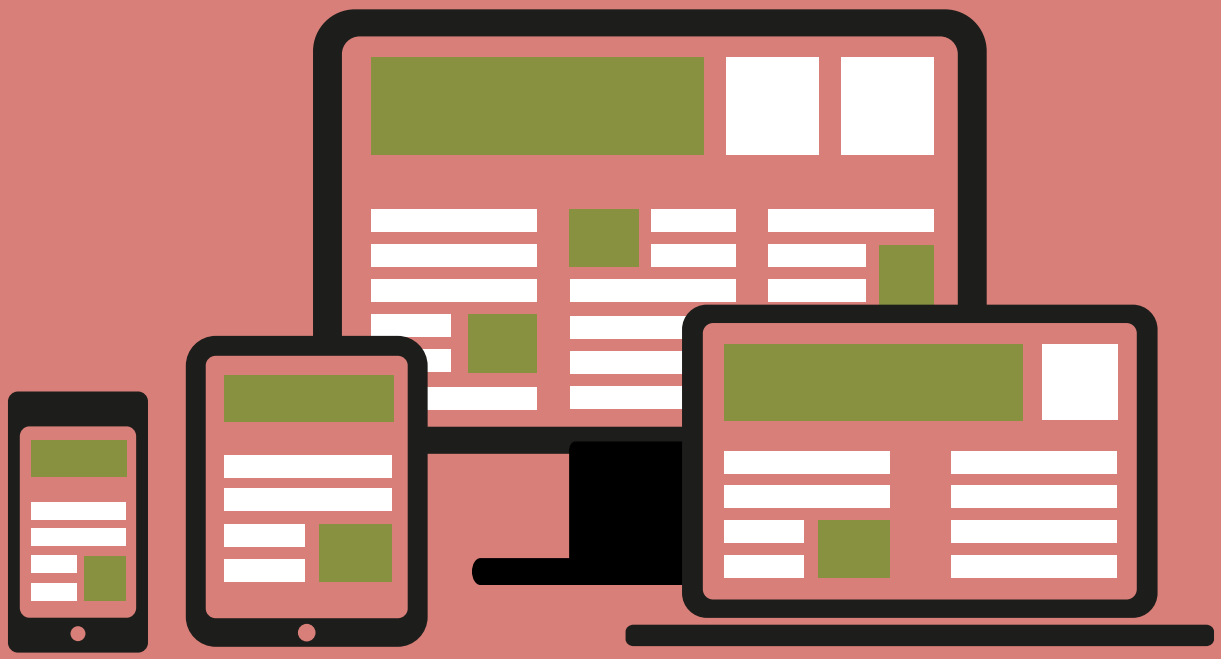
22 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification.

23 COM(2022) 454 final. See https://ec.europa.eu/newsroom/dae/redirection/document/89543.

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit **competitionpolicyinternational.com** today to see our available plans and join CPI's global community of antitrust experts.



CPI COMPETITION POLICY® INTERNATIONAL