The Thinking Watermill Society

Survey

European legislation on cybersecurity

Daniele Redivo

Survey

The Thinking Watermill Society

European legislation on cybersecurity

I. BRIEF DESCRIPTION OF THE SURVEY

This survey aims to describe the past European legislation on cybersecurity, in particular its directives and regulations. For each single legislation, a brief summary of its content will be outlined.

The term ‘cybersecurity’, from an EU perspective, entails a combination of cyber resilience, cybercrime, cyberdefence, strictly cybersecurity and global cyberspace issues.

II. EU CYBERSECURITY LEGISLATION

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems

This Directive introduces new rules harmonising criminalisation and penalties for a number of offences directed against information systems. The main types of criminal offences covered by this directive are attacks against information systems, ranging from denial of service attacks designed to bring down a server to interception of data and botnet attacks.

EU countries must:

a. have an operational national point of contact;
b. use the existing network of 24/7 contact points;
c. respond to urgent requests for help within 8 hours to indicate whether and when a response may be provided;
d. collect statistical data on cybercrime.

Regulation (EU) 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) (The EU Cybersecurity Act)

This Regulation establishes a European Union Agency for Network and Information Security (ENISA) to undertake tasks for the purpose of contributing to a high level of network and information security within the Union, in order to raise awareness of network and information security and to develop and promote a culture of network and information security in society for the benefit of citizens, consumers, enterprises and public sector organisations in the Union, thus contributing to the establishment and proper functioning of the internal market.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data

The Regulation contains provisions and requirements related to the processing of personal data of individuals who are located in the European Economic Area (EEA), and applies to any enterprise, regardless of its location and the data subjects' citizenship or residence, that is processing the personal information of individuals inside the EEA.

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 (NIS Directive)

It provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:

a. Member States' preparedness, by requiring them to be appropriately equipped. For example, with a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority;
b. cooperation among all the Member States, by setting up a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States
c. a culture of security across sectors that are vital for our economy and society and that rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.

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, repealing Regulation (EU) No 526/2013 (The EU Cybersecurity Act)

This Regulation lays down:

a. objectives, tasks and organisational matters relating to ENISA (the European Union Agency for Cybersecurity);
b. a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union.

Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (NIS 2)

In December 2020, the European Commission proposed a revised NIS Directive (NIS2) to replace the 2016 Directive. The new proposal responds to the evolving threat landscape and takes into account the digital transformation, which has been accelerated by the COVID-19 crisis.

The new rules will:

a. strengthen security obligations for companies
b. address the security of supply chains
c. introduce more stringent supervisory measures for national authorities
d. further increase information sharing and cooperation

The Council has reached a general approach on the new directive in December 2021

III. FURTHER SCOPE FOR LEGISLATION

It is now established that a highly fragmented legal framework constitutes the European cybersecurity policy area and that this area is bound to develop further given the EU's digital dependency.

One major point debated within the field of data protection regards the responsibility for ensuring the rights of individuals in the online environment. The current liability framework dates back from the Rome Convention and does not address complex issues as embedded systems, embedded software and application software.

Daniele Redivo	
	Daniele is a student with strong multicultural background, a keen interest for politics and global affairs as well as academic experience in IB diploma. He is currently attending the last year of Political Science and International Relations undergraduate studies at La Sapienza University in Rome.