Summary

Katarzyna Chałubińska-Jentkiewicz

An area that has been partially regulated by law, and one that has special prominence in law systems, is cybersecurity. Cybersecurity needs to be considered as an interdisciplinary concept that draws on multiple fields, including various domains of law. But in order to distinguish it from the legal and administrative system as a whole (in relation to the latter especially in organisational and objective terms), and to categorise it and identify regulatory areas, it is necessary to define the scope of activity that this sphere involves (in subjective, objective, functional and organisational terms). Only then will it be possible to systematise the issue of the legal protection of cyberspace.

When addressing issues related to cybersecurity, in addition to the analysis of systemic solutions, it is important to consider the following questions: What is cyberspace, generally speaking, and how are we responsible for any actions within it? and What legal regulations have so far been adopted within national and international law? How are these enforced and is it correct for these to be based on the regulations concerning reality? What is cybercrime? What are the powers of the organisations responsible for fighting cyber crime?, and, by extension, What are the rights and responsibilities of actors operating in cyberspace, and also Are network users responsible for their online actions? Are they responsible jointly and severally with service providers? And also, How should we balance individual interests, including the right to privacy, and the public interest, which involves actions related to defining responsibility for online actions. The backdrop for these problems are such issues as current strategic and regulatory policies for cyberspace, and the related security challenges and legal regulations to ensure a secure cyberspace.

Ensuring cybersecurity in the EU requires a new policy for prosecuting and penalising individuals and organisations found guilty of breaching communication

K. Chałubińska-Jentkiewicz (✉)

Akademickie Centrum Polityki Cyberbezpieczeństwa/Academic Center for Cybersecurity Policy, Akademia Sztuki Wojennej w Warszawie/War Studies University in Warsaw, Warsaw, Poland

e-mail: k.jentkiewicz@akademia.mil.pl

and information systems. The introduction of new, more effective, solutions, including a review of Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, and also the provisions of the EU's new Cybersecurity Strategy, should be accompanied by a serious discussion on how to strengthen law enforcement authorities at the EU and national levels.

Relevant data shows the need to take action. In 2018, the CERT Polska team received 19,439 security reports and recorded 3739 security incidents, which corresponds to an increase in incident number by 17.5% compared to 2017. In 2019 CERT Polska (CSIRT NASK) recorded 6484 such incidents. This means a massive increase in incidents—by 73% compared to 2018. In the first half of 2020 CSIRT NASK received as many as 16,689 reports, of which 5205 were considered incidents, so the number of incidents in 2020 could be twice as that in 2019. The data presented in CSIRT ABW reports are also alarming. In 2018 CSIRT ABW received 31,865 reports, of which 6236 were considered incidents, and in 2019 there were 226,914 reports, of which 12,405 were considered incidents.

The proposal for the new directive, known as NIS 2, is the product of a review of the currently applicable NIS Directive and is to be part of a broader package including also separate regulations for financial institutions (Regulation on Digital Operational Resilience for the financial Sector, or DORA) and the Resilience of Critical Entities Directive.

It seems that the legislation currently in force is producing certain divergences between individual Member States in relation to the regulated matter. And one of the by-products of this is the lack of restriction instruments to enforce this law against the regulated entities, which significantly undermines cybersecurity. The decision to adopt the new directive seems to be the right thing to do. The new directive will be a minimum harmonisation one, which allows Member States to take further steps to introduce solutions for a higher level of cybersecurity (see Article 3). The proposal provides for the establishment of a Cooperation Group (Article 12) and CSIRTs network (Article 13), and the European Cyber Crises Liaison Organisation Network (EU – CyCLONe) to support the management of large-scale cyberincidents and crises (Article 14). This is crucial due to the extra-territorial nature of these. In the context of 5G network construction, but not only, it is important to introduce provisions on coordinated supply chain risk assessments (Article 19 and Section 47 of the Preamble) and certification schemes (Article 21). Important elements of the directive are also standardisation (Article 22) and information-sharing (Article 26). Without a doubt these areas will affect market activities. While the Commission will decide which categories of key entities (and this status can be held by public entities and private entities which perform public tasks or their own tasks) will be required to obtain certification, the new obligations under NIS 2 will require the involvement of various entities in areas that have not been covered by such regulations. However, certification should apply to device manufacturers rather than entities providing services based on such devices. Political considerations concerning the provenance of the entities selling such devices on the market should not affect the operations of electronic communication services providers. If the

certification obligation is imposed on manufacturers, service providers and network operators will not have to recall the equipment, which can be costly, and manufacturers will need to ensure appropriate manufacturing conditions. With the digitisation and computerisation of the economy, cybersecurity is becoming crucial for more and more fields. And this generates new responsibilities for a new group of entities—important entities. Not everyone will be happy about this, but these regulations are not about market-oriented reforms. The public interest does not always go hand in hand with individual or economic interests.

Whatever their size, businesses providing electronic communication services will need to comply with NIS2 regulations. The directive also provides for heavy fines for entities that fail to appropriately meet their obligations. Maximum fines are to be up to EUR 10,000,000 or 2% of the business' total annual global revenue, whichever is higher. These fines can be particularly painful for smaller businesses which are only entering the cybersecurity system. Perhaps some graduation of fines would be useful here. In order to answer the question about whether this new directive meets market requirements, it is necessary to remember what was the primary goal behind these provisions. And this goal was extensive cooperation between different sectors to ensure cybersecurity. Cybersecurity-oriented actions of Member States and their public authorities, taken within the common and uniform telecommunications market, need to be supported by all its actors. This is also required from telecommunications businesses and all other entities whose operations could or do affect cybersecurity. Without such cooperation and coordination there can be no safe and secure cyberspace.

What is problematic about these solutions for the telecommunications market is that the amended Directive can possibly create collisions with the provisions of other regulations, such as Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, which also addresses the security of electronic communications networks and services, and, in practice, those requirements have been in place for many years. However, it is also important to note that requirements imposed by telecom regulations are one thing, and requirements related to the establishment of a uniform cybersecurity system with the national administration system are another. But it is worth emphasising that new cybersecurity objectives can cause an increase in business costs among the relevant entities, which can be a valid reason to increase the prices for end users.

Irrespective of the above-mentioned concerns, the new directive can contribute to increased resilience to cyberattacks, provided that it is successfully implemented by Member States. Nevertheless, the key factors to ensure security in cyberspace are risk awareness and education. Man is at the centre of cybersecurity.

Personnel training and acquiring the necessary cybersecurity skills are long-term processes, and this needs to be taken into consideration when designing and implementing any cybersecurity mechanisms and requirements. Member States need to become actively involved, also by allocating sufficient funds for this purpose in their budgets, in building professional education about, and training in,

cybersecurity, while closely cooperating with businesses to ensure that the system provides a sufficient number of job candidates with in-demand skills.

Despite all disappointments, failures and tragic mistakes, people will build a better world. If they were not to act with that thought, we would lose all faith in humanity and its potential, in which case it would be better not to live at all my friends.

*Stanisław Lem, Dialogues*¹

Katarzyna Chałubińska-Jentkiewicz dr. hab. of legal sciences (University of Warsaw and the Jagiellonian University), legal advisor, associate professor, and head of the Department of Cybersecurity Law and New Technologies at the Institute of Law in the Faculty of National Security at the War Studies University in Warsaw. She is also a lecturer at the SWPS University and director of the Academic Center for Cybersecurity Policy. In the years 1996–2010, she worked as a lawyer in the National Broadcasting Council and with the public broadcaster TVP S.A. Between 2011 and 2017, she was deputy director of the National Audiovisual Institute (her competence centered on the field of digitization). As a scientist, she conducts research on cybersecurity, information security threats, the development of electronic media law, protection of intellectual property, and the impact of new technologies on the development of the state and the legal situation of the individual. Katarzyna Chałubińska-Jentkiewicz is the author of monographs and numerous articles, which include topics such as new technologies law, cyber responsibility, information security law, and audiovisual media: Regulatory conflict in the age of digitization, Audio visual media services; Regulation in the conditions of digital conversion; Information and computerization in public administration; Cultural Security Law and Reuse of public sector information. She is head of the Ministry of Science's research project "Polish cybersecurity system – a model of legal solutions."

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

¹Dialogi Wydawnictwo Literackie, Kraków – Wrocław 1984, p. 287.