dott. Federico Serini
PhD in Public, Comparative and International Law
Public Economics Law curriculum
La Sapienza Roma

Market and security in the era of cyber risk. Standards and certifications for ICT security assets between the needs of free trade and national security in the European Union context

Computer resources are essential elements for democracies. These tools not only serve as a means for individuals to freely express their personalities in new forms and ways through the network, but also play a crucial role in facilitating communication, information sharing, and participation in democratic processes[1] but at a technical level[2], they also serve as the configuration and operational parameters of many infrastructures that provide essential services and functions for society and the economy (known as critical infrastructures). Consider the computer systems used by operators in the banking and financial, energy, transportation, communications, and healthcare sectors, as well as those utilised by public administrations and various government institutions.

These tools have become indispensable not only for the State itself but also for its components, primarily individuals and businesses. They play a vital role in facilitating the functioning of various sectors, enabling efficient operations, data management, and communication, ultimately contributing to the overall functioning of society and the economy[3]. However, at the same time, they are also responsible for transferring the risks of cyberspace into the real world. The intention to create a "global network" characterised by the principles of free access and interoperability led to the development of a system that was not designed to adhere to security criteria but rather to principles of open access and information exchange. These principles now clash with the possibilities of dual use[4] of the network and information services, to the point that someone has warned that today «every society is as vulnerable as the information technology it uses" and therefore "the more advanced societies are, the more vulnerable they are»[5].

Despite this condition, according to which "cyber risk = social risk", it highlights how the protection and guarantee of rights and freedoms in today's technological society also depend on the security of networks and computer systems. Ensuring the security of networks and systems is crucial for safeguarding the privacy, integrity, and availability of information, as well as maintaining trust in digital interactions and

[1] V. Frosini, *La democrazia nel XXI secolo* (1997), Macerata, Liberilibri, 2010, pp. 40-41.

[2] C. Gallotti, *Information Security Management Systems The ISO/IEC 27001:2022 standard The controls of ISO/IEC 27002:2022,* Lulu press, 2022.

[3] G. De Vergottini, *Sicurezza e i diritti fondamentali*, in L.E.R. Vega, L. Scaffardi, I. Spigno, *I diritti fondamentali nell'era della digital mass surveillance*, Napoli, Editoriale scientifica, 2021, p. 28.

[4] Dual-use products are products, including software and information technologies, that can have both civil and military uses. Such goods are regulated by Regulation (EU) 2021/821, which establishes a European Union regime for the control of exports, brokering, technical assistance, transit, and transfer of dual-use products.

[5] M.G. Losano, *Guerre ibride, omicidi mirati, droni: conflitti senza frontiere e senza diritto*, in L. Forni, T. Vettor (a cura di), *Sicurezza e libertà in tempi di terrorismo globale*, Torino, Giappichelli, 2017, p. 22. On the effects of connectivity not only due to ICT technologies see A.L. Baràbasi, *Linked. How everything is connected to everything else and what it means for business, science, and everyday life*, New York, Basic books, 2014. Similarly, see also P. Khanna, *Connectography: The Maps of the Future World Order*, Roma, Fazi, 2016.

transactions. It is an integral part of ensuring the overall well-being and functioning of individuals and society in the digital age[6], Public authorities have only recently turned their attention to this phenomenon (more or less starting from the late 1990s), following the increasing dependence on States and infrastructures on information technology.

The demand for security in cyberspace by States now clashes with the effects resulting from this delay. Cyberspace is, in fact, an originally public phenomenon, born with the Arpanet project[7], it was subsequently developed and disseminated by private entities, beyond the control of states[8].

It is not a coincidence that the initial definitions of cybersecurity, computer security, and information security were formulated within the domain of "private law"[9], specifically, they were formulated within technical sector regulations[10].

However, if in the digital environment it seems that there is no longer a State, territory, sovereignty, or even a people, but rather primarily private production of law, it is not solely because public authorities arrived "later," but mainly because the object of regulatory pretension, cyberspace, is a global phenomenon devoid of territoriality. Cyberspace represents a limitation on the action of public power, which, on the other hand, boasts an «original need for places»[11].

In reality, as noted in the literature on this matter[12], cyberspace is a dimension characterised by the coexistence of immaterial components, such as connections, electromagnetic spectrums, and operating protocols, which are not inherently tied to any physical space. It also consists of material components, namely physical technologies like cables, routers, and switches, located within the boundaries of states and typically produced by private actors active in the telecommunications market.

The outlined morphology demonstrates that, in both realms, public action for cyberspace security necessitates necessary cooperation with private entities. Regarding the immaterial profile, this cooperation

[6] Cfr. M. Dunn Cavelty, *Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities*, in *Science and Engineering Ethics,* vol. 20, 2014, p. 704.

[7] M. O'Mara, *The Code: Silicon Valley and the Remaking of America, Londra*, Penguin Press, 2019.

[8] G. Bombelli, *Dal moderno all'"ultramoderno"? Intorno al nesso diritto-tecnica-sicurezza*, in F. Pizzolato, P. Costa (a cura di), *Sicurezza e tecnologia*, Milano, Giuffrè, 2017, p. 26; G. Della Morte, *Big data e protezione internazionale dei diritti umani, regole e conflitti,* Napoli, Editoriale scientifica, 2018, p. 27, Where the author specifies that the Internet is only one region of cyberspace, and therefore the two terms are not synonymous.

[9] With Recommendation ITU-T X.1205, dated April 18, 2008, the International Telecommunication Union (ITU) defined cybersecurity as the set of political, legal, and technological tools aimed at protecting the cyber environment and user assets from cyber risks, particularly ensuring the three priorities of confidentiality, integrity, and availability. Another definition can be found in the technical standard ISO/IEC 27032, where cybersecurity is considered as the action aimed at the «preservation of confidentiality, integrity, and availability of information in the Cyberspace».

[10] H. Schepel, *The Constitution Of Private Governance: Product Standards In The Regulation Of Integrating Markets*, Londra, Hart Pub Ltd, 2005. Regarding the historical evolution of technical standardization in the fields of computer with and information security, see D. Russell, G.T. Gangemi, *Computer security basics*, Sebastopol, O'Reilly Media, 1991, 23.

[11] N. Irti, *Norma e luoghi*, Roma-Bari, Laterza, 2006, p. 4.

[12] According to the scholar F.D. Kramer, there exist 28 different definitions of the term "cyberspace." Refer to F.D. Kramer, S. Starr, L.K. Wentz, *Cyberpower and National Security: Policy Recommendations for a Strategic Framework*, in *Cyberpower and National Security*, Washington (D.C.), National Defense University Press, 2009. Among these, for this discussion, the reference is made to Martin C. Libicki's definition of cyberspace, which identifies three levels: physical, syntactic, and semantic. See M.C. Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica, RAND Corporation, 2009, pp. 11-38.

aims to regulate what occurs "in" cyberspace, including the conduct and behaviours of users, among which we can identify cybersecurity threats. Concerning the material aspect, the aim is to ensure the security "of" cyberspace through the creation and development of market products and solutions that are designed with cybersecurity in mind, ensuring the progressive security of the digital environment[13].

This proposal is part of the Authors' PhD thesis, recently discussed in May (here in open access: https://iris.uniroma1.it/handle/11573/1711004), and wants to reflect on the use of technical standards from the economy to the social/political aims, in light of the regulatory framework outlined by the European Union regarding cybersecurity.

The high level of expertise required in regulating the subject matter and the rapid pace of technological change have led legislators to increasingly delegate regulatory competence to standardization bodies responsible for developing standards in areas heavily influenced by technical and scientific factors[14]. In particular, among these standardization bodies, those focusing on the security of computer resources and information have gained increasing importance due to the close correlation between cyber risk and social risk. The growing significance of computer infrastructures, not limited to critical infrastructures alone, has led these regulatory instruments - originally developed within the private context to contribute to the smooth functioning of the market - to intersect with political and social objectives such as public order and national security of States[15].

The occasion is to reflect on the entry of these non-legal norms, as tools, into the field of (European) cybersecurity, as a new branch of security that arises from the private sector and now engages public law scholars.

[13] A. Vedder, *Safety, Security and Ethics*, in A. Vedder, J. Schroers, C. Ducuing, P. Valcke (eds), *Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*, Cambridge, Antwerp, Chicago, 2019, pp. 11-26, available at:<https://ssrn.com/abstract=3457301>; M. Durante, *Safety and Security in the Digital Age. Trust, Algorithms, Standards, and Risks*, in D. Berkich, M. d'Alfonso (eds), *On the Cognitive, Ethical, and Scientific Dimensions of Artificial Intelligence. Philosophical Studies Series*, vol 134, Springer, 2019, available at:< https://doi.org/10.1007/978-3-030-01800-9_21>.

[14] v. C. Joerges, H. Schepel, E. Vos, *The Law's Problems with the Involvement of Non-Governmental Actors in Europe's Legislative Processes: The Case of Standardisation under the "New Approach"*, in *EUI Working Paper law*, n. 9, 1999. T. Buthe, W. Mattli, *The new global rules: the privatization of regulation in the world economy*, Princeton, Princeton University Press, 2011.

[15] H. Nissenbaum, *Where Computer Security Meets National Security*, in *Ethics and Information Technology*, volume 7, 2005, pp. 61–73.