European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 2, pp. 173-174
ISSN 2724-5969 – ISBN 979-12-218-1266-4 – DOI 10.53136/9791221812664 16

Book Review

Stefano Rossa, *Cybersicurezza e Pubblica amministrazione,* Naples, Editoriale Scientifica, 2023.

Although it is not a novelty in the global legal landscape, the issue of cybersecurity has acquired a clear centrality in the political and legal debate of recent years, as shown by the important legislative and institutional initiatives taken both at the European and national level.

Stefano Rossa's work fully grasps this centrality and demonstrates full awareness of the importance of understanding and adequately managing the exponential increase in cyber threats linked to the spread of cyberspace. Cyber threats can be distinguished following different criteria, such as those related to the purpose of the attacks or their mode of operation. However, among the others, the criterion of the target-subject of the criminal action has a particular importance. In fact, in the event that a cyber-attack is aimed at a private subject, the effects of such action will be borne by the private subject affected and its possible suppliers; on the contrary, in the event that the cyber-attack is aimed at a public entity, the interests of the community will be endangered, as if the attacker intends to damage or disrupt the crucial digital infrastructures on which the functioning of democratic authorities depends.

The author chooses to direct his scientific investigation on the specific needs of prevention and protection against cyber risk warned by public administrations, which are increasingly victims of intense and potentially devastating cyber-attacks, as underlined by the data collected by the Italian Information System for the Security of the Republic (p. 20).

The book is divided into six chapters and can be divided into three parts.

In the first part, the Author reconstructs and analyzes the concept of "public cybersecurity", underlining the most significant issues arising for the proper conduct of the action of public administrations. Among the various critical issues, those relating to the ownership and the management of digital infrastructures stand out, since it depends on them the exercise of many administrative functions and the provision of important public services in favor of the community.

In fact, due to the affirmation of an increasingly digitalized economic and social context, public authorities are now in a situation of considerable weakness and dependence on large private companies (the so called "Big tech") providing the technology necessary to carry out their institutional functions. This situation has led to several negative consequences in recent years, such as the constant need for public authorities to update themselves on the new cyber threats of the Internet and on the most effective tools to combat them, but also the increasing need for public bodies to turn to the ICT market to purchase goods and services of cybersecurity.

In order to provide a clear overview of the recent multi-level regulatory discipline, the second part of the work deepens the aforementioned notion of public cybersecurity under a dual meaning.

The first meaning is that of "vertical cybersecurity", which concerns the institutional relations established between the different levels of government involved (European and national).

In this part the Author dwells on the legal architecture devised in Europe to prevent and combat cyber threats, underlining the significant role and the new attributions recently assigned to ENISA (the *European Network and Information Security Agency*). While this European authority is certainly the main reference point in the field of cybersecurity within the Union, not least in view of its important advisory and operational tasks, the importance of the European Agency must be considered, as Rossa points out, for its fundamental connection activity between the different European bodies and those of the Member States (in Italy, mainly the *National Cybersecurity Agency* or ACN). This organizational model entails the creation of a real "decentralized star network" (p. 100), in which each node of the network has a different function and responsibility, albeit under the constant coordination and support of ENISA.

The second meaning outlined in the work is that of "horizontal cybersecurity", which concerns, instead, the relationship between all the subjects, public and private, involved in the prevention and counteraction of cyber risks.

In this regard, the author points out in critical terms that the choices of regulation undertaken so far at the European and Italian level have been mainly inspired by a very authoritative logic (summarized in the binomial "obligation-sanction"), as shown by the provisions relating to the introduction of new, rigid bureaucratic requirements for market enterprises: *i)* adopting minimum technical measures, *ii)* reporting obligations for cyber incidents, *iii)* complying with the common framework for the certification of digital goods and services (p. 111 ff.).

In particular, this authoritative logic finds expression in the moment of the purchase of goods and services of cybersecurity from the public contracting stations: an operation still realized through the use of traditional procedures of choice of the contractor, characterized by excessive formalism (such as the "open public procedures").

Indeed, the same intrinsic characteristics of the concept of public cybersecurity demonstrate the importance of combining a top-down regulatory and operational approach with a more collaborative approach between public authorities and private actors, including with a view to enhancing the effectiveness and quality of national public-sector IT security policies.

Starting from the above-mentioned conceptual coordinates and the practical criticalities, the third part of the analysis emphasizes the opportunity to promote the widening of the limited spaces of collaboration existing inside our legal system with reference to the relationship between public and private actors. According to Rossa, this objective can be concretely and effectively achieved not only through the dissemination of a solid cyber security and ICT culture (both among administrative officials and civil society), but also through the application of legal institutions more suited to the peculiarities of the technological market, such as that of "innovative procurement".

In particular, the increased use of innovative procurement (especially in the case of "innovation partnership") would allow public authorities to pursue two key advantages.

Firstly, public administrations could regain negotiating and strategic autonomy from private technology suppliers, establishing a dialogue with them aimed at the choice and the development of quality digital goods and services, designed to be "by design" aimed at satisfying public interests. From this perspective, as the Author points out, "the contracting entity avoids being captured by the technology provider: it is aware of its needs and how to obtain them in synergy with the operator" (p. 205).

Secondly, the tool of innovative procurement would enable national authorities to exercise a genuine planning function, through which it would be possible to pursue the ultimate objective of protecting the cybersecurity of all digital networks and infrastructures used for public purposes. In fact, by using these innovative types of purchasing tools, the public buyer and the private technology suppliers could collaborate in the design, prototyping and marketing of the established ICT goods or services, creating a sort of "oriented collaboration" (p. 210) consistent with the principles of result, trust, and good faith enshrined in the new Italian Code of public contracts (legislative decree no. 36/2023).

Highlighted the need to wisely combine the authoritative logic with the collaborative one in the field of cybersecurity, the concluding remarks of the author underline the urgency for a reaffirmation of the role of the State, as a guide and promoter of national technological development, according to the model of the "Entrepreneurial State" theorized by the economist Mariana Mazzucato (see *The Entrepreneurial State. Debunking Public vs. Private Sector Myths*, Anthem Press, London, 2013).

It is only through this approach, in fact, that it will be possible to build a symbiotic ecosystem in the sector of cybersecurity, based on cooperative relations between public and private subjects, in which the solutions and tools to be used will not be the result of top-down decisions, but bottom-up strategies, in order to better pursue the interests of the community (reviewed by LUIGI PREVITI).