ADMINISTRATIVE LAW REFLECTIONS ON CYBERSECURITY, AND ON ITS INSTITUTIONAL ACTORS, IN THE EUROPEAN UNION AND ITALY

Stefano Rossa[*]

Abstract

This paper offers some reflections on administrative law dedicated to the field of cybersecurity. After reconstructing the European and national discipline of institutional actors operating in this area, in particular the ENISA and the Italian *Agenzia per la Cybersicurezza Nazionale*, the paper investigates the relationship between these two bodies. In the conclusion, the analysis highlights the need for a cybersecurity model characterized by a broader participation of non-institutional actors, also with the benefit of more institutional sustainability.

TABLE OF CONTENTS

1. Introduction. Hybrid Warfare and Cybersecurity: Digital Attacks with Real Effects

The etymology of the Italian word '*guerra*' (war) reveals how it has traditionally been fought with boots on the ground. As

[*] Assistant Professor of Administrative law, University of Eastern Piedmont

has been observed[1], the word 'war' derives from the Germanic word '*werra*', which had the meaning of scrum, scuffle, confusion, and was in contrast to the Classical Latin lemma '*bellum*', a term that had a more strategic connotation related to the manoeuvres of armies. 'War', therefore, emphasises how, from the earliest times, conflicts were resolved directly on the battlefields where soldiers fought hand-to-hand.

Over the years, technology applied to warfare[2] has allowed soldiers to physically distance themselves from the enemy while increasing their own offensive capacity – and conversely, the opponent's defensive capacity. Consider that, historically, in the beginning, people fought with sticks and swords, then they moved on to bows and arrows, then to guns and cannons and, most recently, to jets, missiles, and drone bombers.

Military technology, which has also enabled great advances in the civil sphere[3], has undergone strong development particularly since the 20th century and this exponential growth – in accordance with Moore's Law[4] – has not yet stopped. With the increase in the technological level of military equipment, the physical distance with which warfare can be carried out with the aid of ICT has increased in parallel. This is due to the increased ability to collect data, process it into information and use it as an advantage in war contexts, with the simultaneous need to protect communication systems[5].

---

[1] Cf. G. Moretti, *Il lungo viaggio delle parole*, 40/158 Prometeo. Rivista trim. di scienze e storia 59 ss. (2022).

[2] On the relationship between anthropology and technology, see A. Gehlen, *Man in the Age of Technology* (1980), in which this Author highlights how technology can be both an evolutionary factor but also a potential weapon.

[3] For instance, the development of GPS which born for military purposes and then adopted in everyday life. Internet itself was developed as a result of the ARPANET (Advanced Research Projects Agency NETwork) project in 1969. Over the years, ARPANET would take on the current architecture of the Internet thanks to the subsequent development of the TPC (Transmission Control Protocol) and IP (Internet Protocol) protocols that would enable the various networks to be interconnected.

[4] Moore's law is an empirical law according to which the computing performance of transistors doubles every eighteen months. Cf. C. Mody, *The Long Arm of Moore's law: Microelectronics and American Science* (2016).

[5] In relation to the link between the security of military communications and the human factor, see the interesting considerations of A. Kerckhoffs, *La cryptographie militaire*, vol. IX, Jan.-Febr. Journal des sciences militaires 5 ss. and 161 ss. (1883).

Modern conflicts have become hybrid wars, fought with both 'traditional' weapons and 'non-traditional' tools, both in a 'traditional' environment such as the battlefield and in a 'non-traditional' environment such as cyberspace. The recent Russian-Ukrainian[6] conflict has highlighted this point, especially in relation to cybersecurity, aimed at preventing cyberattacks that represent a veritable additional weapon of war capable of striking enemy nerve centres at a distance. A digital weapon with tangible consequences in the physical world[7].

2. Topic Outline Fundamental Concepts

This paper proposes to investigate the administrative law implications of cybersecurity policies adopted in the European Union, in particular by analysing the actions of the main institutional actors operating in this field at EU level and at the Italian level.

Before proceeding with the discussion, it is necessary to briefly clarify what is meant by cybersecurity, since this concept is rather broad and intricate, especially from a technical point of view[8].

Cybersecurity is a made up word, composed by the confix 'Cyber' and the suffix 'Security'.

On the one hand, 'Cyber' derives from the ancient Greek expression '*cybernetiké*' used by Plato in Gorgias to indicate 'the art of piloting ships'[9]. Over the ages, particularly since the second half of the 20th century, a number of scientific theories developed that emphasised the link between communication, society and law (as the Wiener's Cybernetics)[10]. From there on, the word 'cyber' was automatically linked to everything to do with IT and digital. And

---

[6] For an geopolitical analysis, among numerous contributions, see in Italian P. Sellari, *Il conflitto russo ucraino: una visione geopolitica*, 17 federalismi.it 4 ss. (2022) and E. Chiti, *Guerra e diritto amministrativo*, 3 Gior. dir. amm. 293 ss. (2022).

[7] On the subject, in a broad sense, L. De Nardis, *The Internet in Everything. Freedom and Security in a World with No Off Switch* (2020).

[8] Cfr. European Union Agency for Network and Information Security (ENISA), *Definition of Cybersecurity. Gaps and overlaps in standardisation* (2015) in https://bit.ly/3cLuHbg [last cons.: 06.08.2022].

[9] Cf. A. Taglia (ed.), *Gorgias, Platone* (2014), v. 511.

[10] For instance the Cybernetics by Norbert Wiener. Cf. N. Wiener, *Cybernetics: or Control and Communication in the Animal and the Machine* (1948).

this is also thanks to William Gibson, an exponent of the Cyberpunk literary current who indirectly reinforced this relationship by inventing the term 'Cyberspace' in his book Neuromancer[11].

On the other hand, the suffix 'Security' refers to those organized activities aimed at protecting people or goods from danger or damage. Security is the organisational means to achieve safety.

In the light of what outlined above, it is possible to affirm that cybersecurity means a technical-organisational system aimed at protecting the IT infrastructures of complex public (e.g. the State, government structures, public administrations, etc.) or private (e.g. companies) organisations from cyberattacks. This paper will focus on cybersecurity related to the public sector, where actions are taken to counter cyberattacks that may be a threat to national security: either because they target crucial state infrastructures or because they aim to block the supply of essential services. The discussion, however, will not focus on criminal law aspects, although the field of cybercrime is intricately linked to that of cybersecurity in the proper sense of the term. Therefore, the paper will focus on the analysis of the institutional actors operating in the cybersecurity context, namely ENISA in the EU and the *Agenzia per la Cybersicurezza Nazionale* (ACN) in Italy, and the effects of their relationship.

3. The European Union Agency for Cybersecurity (ENISA) in the Context of the EU Cybersecurity Framework

Sun Tzu, in his work *The Art of War*, warns the reader that to win a battle it is not enough to know the enemy, but that it is imperative to know oneself[12]. According to the Chinese masterpiece, to win it is necessary to prepare a defence system,

[11] Cf. W Gibson, *Neuromancer* (1984).

[12] Cf. S.B. Griffith (transl.), *Sun Tzu*, *The art of war*, III, 30-33, 84 (1963): «[i]t is in these five matters that the way to victory is known. / Therefore I say: 'Know the enemy and know yourself; in a hundred battles you will never be in peril. / When you are ignorant of enemy but know yourself, your chances of winning or losing are equal. / If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril'».

centred on the neutralisation of enemy attacks, that derives from an effective internal tailor-made organisation.

At the beginning of the new millennium, the EU institutions set up some agencies[13] tin order to prevent and fight the crime on European territory. Among them the European Police Office (so-called Europol, based in The Hague), the European Union Agency for Law Enforcement Training (so-called CEPOL, based in Budapest) and the current European Border and Coast Guard Agency (so-called Frontex, based in Warsaw).

The European Union also acted cybersecurity area mainly through two agencies: the Europol and the European Network and Information Security Agency (so-called ENISA, based in Athens), today known as EU Agency for Cybersecurity[14]. Europol acts in particular in the criminal sphere, thanks to the creation in 2013 of the European Cybercrime Centre (c.d. EC3)[15] a special division dedicated to the contrast and prevention of cybercrimes, including those committed in the so-called Dark Web, in particular cyber-dependent crime, child sexual exploitation and payment fraud. ENISA, however, operates on the cybersecurity side properly, from a technical policy implementation viewpoint. As previously underlined, this paper will not dwell on the criminal aspects, which is why the following discussion will be dedicated to the analysis of ENISA without focusing on Europol.

ENISA was created by Regulation (EC) 2004/460[16], as the European institutions had become aware of the need to ensure an adequate level of protection of communication networks and information systems throughout the European Union[17]. In fact, at that time, the proper functioning of communication networks was

---

[13] About this topic, see *ex multis* E. Chiti, *European Agencies' Rulemaking: Powers, Procedures and Assessment*, European Law Journal 93 ss. (2013); M. Busuioc, *European Agency: Law and Practices of Accountability* (2013); M. Chamon, *EU Agencies. Legal and Political Limits to the Transformation of the EU Administration* (2016); F. Coman-Kund, *European Union Agencies as Global Actors* (2018); in Italian J. Alberti, *Le agenzie dell'Unione europea* (2018).

[14] The ENISA institutional website is https://www.enisa.europa.eu/ [last cons.: 06.08.2022].

[15] About it see https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 [last cons.: 06.08.2022].

[16] The text of Regulation (EC) 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency can be consulted at https://bit.ly/3PFvAAP [last cons.: 06.08.2022].

[17] Cf. Article No. 1 Regulation (EC) 460/2004.

a crucial factor for social, competitive and economic development[18].

Regulation (EC) No. 460/2004 had delineated ENISA as an agency with limited tasks, as these were purely of a technical advisory nature, for the benefit of the Member States, in the field of cybersecurity[19]. For this reason, the Regulation had provided for ENISA to have a limited duration of five years[20].

The rapid technological development, and the consequent increase in its pervasiveness on society, led to an increase in cybersecurity risks. For this reason, in this field the European legislator approved new legislation[21] and implemented previous frameworks such as the one establishing ENISA[22]. The goal was clear: to make the European Union cybersecurity system more resilient and functional than before. One of the most significant new regulations introduced is Regulation (EU) 2019/881 (the so-called Cybersecurity Act) [23].

---

[18] Cf. whereas No. 1), 2) and 3) Regulation (EC) 460/2004.

[19] Cf. Articles No. 2 and 3 Regulation (EC) 460/2004.

[20] Cf. Article No. 27 Regulation (EC) 460/2004.

[21] Cf. 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 – s.c. NIS (*Network and Information Security*) Directive. The text can consulted in at https://bit.ly/3PFr0Ct [last cons.: 06.08.2022]. The latter directive established the Computer Security Incident Response Team (CSIRT), an intervention group that takes action in the event of a computer security compromise. There is currently a proposal to revise the NIS Directive with a view to issuing the s.c. NIS 2 Directive, which if approved could have a broader application range than the NIS directive, particularly with regard to its notification obligations. See E. Biasin, E. Kamenjašević, *Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals*, 3 Int. Cybersec. Law Rew. 163 ss. (2022).

[22] *Ad exemplum* Regulation (EC) 1007/2008, Regulation (EU) 580/2011 and the Regulation (EU) 526/2013. Among the most significant amendments, it is worth noting the continued extension of the Agency's duration.

[23] The 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 and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) can be consulted at https://bit.ly/3vlYQVf [last cons.: 06.08.2022]. Cf. also the Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade, 16.12.2020, JOIN(2020) 18 final 2020 in https://bit.ly/3cOH5an [last cons.: 06.08.2022]. See *multis* A. Mitrakas, *The emerging EU framework on cybersecurity certification*, 7 Datenschutz und Datensicherheit 411 ss. (2018); C. Kohler, *The EU Cybersecurity Act and the*

To achieve this purpose, the Cybersecurity Act operated on two fronts. On the one hand, by redefining the competences and organisation of ENISA. On the other hand, by introducing a common EU cybersecurity certification system for ICT products – protecting the consumer and competition[24] by providing for mutual recognition of cybersecurity certificates of the national authorities of the various Member States[25].

Focusing on the first aspect mentioned above, as a result of the Cybersecurity Act, ENISA acquires a new central role in EU cybersecurity policy, becoming a proper «centre of network and information security expertise for the EU, its member states, the private sector and EU citizens»[26].

This is not only in view of the 'extension' of its duration from temporary to permanent[27], but especially in relation to its new tasks. The mandate given by the Cybersecurity Act to ENISA is twofold. On one side, to create a «a high common level of cybersecurity across the Union, including by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity»[28]. On the other side, to reduce fragmentation in the European internal market for cyber security by promoting an EU cybersecurity policy[29].

European Standards. An Introduction to the Role of European Standardization, 1 Int. Cybersec. Law Rew. 7 ss. (2020). Recently Z. Bederna Z. Rajnai, *Analysis of the cybersecurity ecosystem in the European Union*, 3 Int. Cybersec. Law Rew. 35 ss. (2022).

[24] In fact, as stated in Whereas 67) Regulation (EU) 2019/881, national certification systems of individual EU Member States are often not recognised outside the borders of the single national state. In order to participate in cross-border tenders, economic operators are therefore forced to turn to private certifiers, resulting in higher product or service costs. In addition, according to the Cybersecurity Act, such private certifications do not always present homogenous levels of reliability, to the detriment of the principle of equal competition. For contingent reasons, this paper will not analyse the common European cybersecurity certification system.

[25] It should be underlined, however, that Regulation (EU) 2021/887 of 20 May 2021 established the European Cybersecurity Competence Centre, based in Budapest, which will not be analysed in this paper.

[26] European Union Agency For Network and Information Security, *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity* 1 (2018), in https://bit.ly/3yOc0MI [last cons.: 06.08.2022].

[27] Cf. Article No. 68 Regulation (EU) 2019/881.

[28] Cf. Article No. 3 Regulation (EU) 2019/881.

[29] *Ibidem*. As highlighted by F. Campara, *Il Cybersecurity Act*, in A. Contaldo, D. Mula (eds.), *Cybersecurity Law* 73 (2020), the Court of Justice of the European

To that that, the tasks assigned to ENISA concern specific types of activities: (1) the assistance to EU institutions, bodies, offices and agencies, as well as to Member States, in the development and implementation of Unional policies relating to cybersecurity, including through technical support actions[30]; (2) the operational cooperation, coordination and sharing of information relating to cybersecurity at EU level between Member States, EU institutions, bodies, offices and agencies, and public and private sector stakeholders, as well as between the European Union, third countries and international organisations[31], including by coordinating actual international cybers exercises[32]; (3) the development of skills and knowledge in the field of cybersecurity[33]; (4) the promotion and the development of the EU policy on cybersecurity certification of technological products and services[34].

From the tasks and competences expressly given to ENISA by the Cybersecurity Act[35], it appears that it is no longer merely a EU technical advisory agency, but a proper operational agency in the field of cybersecurity[36].

Union had already ruled favourably on ENISA's role of promoting common European policies in support of the European internal market in favour of the member states. Cf. Court of Justice of the European Union (Grand Chamber), 2 May 2006, United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union (C-217/04), in https://bit.ly/3zESKlp [last cons.: 06.08.2022].

30 Cf. Article No. 4 and 5 Regulation (EU) 2019/881. According to Articles No. 62 par. 5 and 22 par. 4 Regulation (EU) 2019/881, ENISA is responsible for assisting the European Commission in the secretariat functions of the European Cybersecurity Certification Group (ECCG), as well as in the secretariat functions of the Stakeholder Group for Cybersecurity Certification (SCCG).

31 Cf. Articles No. 4, 7, 9 and 12 Regulation (EU) 2019/881.

32 Cf. the ENISA official website at https://www.enisa.europa.eu/topics/cyber-exercises [last cons.: 06.08.2022].

33 Cf. Articles No. 4 and 6 Regulation (EU) 2019/881.

34 Cf. Articles No. 4, 8, 10 and 11 Regulation (EU) 2019/881.

35 It seems necessary to mention that, according to Articles No. 13 to 28 Regulation (EU) 2019/881, ENISA's administrative structure is composed of five figures: the Management Board; the Executive Committee; the Executive Director (currently Estonian Juhan Lepassaar); the Advisory Group; and the network of national liaison officers.

36 In this sense, in Italian, also R. Brighi, P.G. Chiara, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, 21 federalismi.it 24 (2021), and F. Campara, *Il Cybersecurity Act*, in A. Contaldo, D. Mula (eds.), *Cybersecurity Law*, cit. at 29, 72.

As it is easy to deduce, the cybersecurity has impacts on numerous other subjects and in various contexts. For this reason there is a need to standardise as much as possible the legal discipline of the various Member States (despite the fact that there are some areas that are still the exclusive competence of the member states, such as the operational management of cyber incidents[37]). For this reason, each EU State is required to have a national cybersecurity discipline and appropriate bodies, in accordance with the provisions of Directive 2016/1148/EU[38].

In fact, for instance, in France there is the *Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI)[39], in Germany the *Bundesamt für Sicherheit in der Informationstechnik* (BSI)[40], in Spain the *Instituto Nacional de Ciberseguridad* (INCIBE)[41], in Portugal the *Centro Nacional de Cibersegurança* (CNCS)[42], in Ireland the National Cyber Security Centre (NCSC)[43], in Belgium the Centre for Cyber Security Belgium[44], in the Netherlands the *Nationaal Cyber Security Centrum*[45], in Denmark the C*enter for Cybersikkerhed*[46], in Sweden the *Nationellt cybersäkerhetscenter*[47]. In Italy, instead, the *Agenzia per la Cybersicurezza Nazionale* (ACN) has been recently established[48]

4. The Italian *Agenzia per la Cybersicurezza Nazionale* (ACN) and the Italian Cybersecurity Framework

Under the impulse of EU law[49] the Italian government, headed by Mario Draghi, in the summer of 2021 set up the *Agenzia per la Cybersicurezza Nazionale* (henceforth, ACN).

---

[37] In this way, in Italian, L. Tosoni, *Cybersecurity Act, ecco le nuove norme in arrivo su certificazione dei prodotti e servizi ICT*, Agenda digitale.eu. (2019).
[38] Cf. Articles No. 7 and 8 Directive (EU) 2016/1148.
[39] The institutional website is https://www.ssi.gouv.fr/ [last cons.: 06.08.2022].
[40] The institutional website is https://www.bsi.bund.de/DE/Home/home_node.html [last cons.: 06.08.2022]. In the BSI there is the *Cyber-Sicherheitsrat*.
[41] The institutional website is https://www.incibe.es/ [last cons.: 06.08.2022].
[42] The institutional website is https://www.cncs.gov.pt/ [last cons.: 06.08.2022].
[43] The institutional website is https://www.ncsc.gov.ie/ [last cons.: 06.08.2022].
[44] The institutional website is https://ccb.belgium.be/ [last cons.: 06.08.2022].
[45] The institutional website is https://www.ncsc.nl/ [last cons.: 06.08.2022].
[46] The institutional website is https://www.cfcs.dk/ [last cons.: 06.08.2022].
[47] The institutional website is https://www.ncsc.se/ [last cons.: 06.08.2022].
[48] The institutional website is https://www.acn.gov.it/ [last cons.: 06.08.2022].
[49] And this both in relation to the national implementation of the European framework expressly mentioned in the previous paragraph, and in relation to

The legal framework establishing the ACN is provided by Decree-Law No. 82/2021 (converted with some amendments into Law No. 109/2021)[50]. This framework represents only the last piece of the mosaic of the Italian cybersecurity legislation, which arose first with Legislative Decree No. 65/2018[51] – implementing Directive 2016/1148 – and subsequently continued with Legislative Decree No. 105/2019 (converted into Law No. 133/2019)[52] establishing the national cybersecurity perimeter (in Italian *perimetro di sicurezza nazionale cibernatica* – PSNC)[53].

In relation to the PSNC, which for reasons of economy of exposition we do not have the opportunity there to analyse in detail, it is only sufficient to mention that it is a unique and avant-garde instrument in the panorama of the various national cybersecurity frameworks. The perimeter consists of a legal framework within which particular cybersecurity regulations are applied to two specific categories of actors: public or private entities exercising an essential function of the State or providing a public service essential to the maintenance of civil, social or economic activities fundamental to the interests of the State[54]. Of course, this public function or service must depend on information-digital networks or systems[55] from the malfunction,

---

the Next Generation EU, adopted at the extraordinary European Council of 17 and 18 July 2020, the substantial programme of investments (as much as 750 billion Euro) and reforms aimed at accelerating the digital and ecological transition in order to revitalise the economies of the member countries deeply damaged by the crisis caused by the pandemic. Thanks to the National Recovery and Resilience Plan (*Piano Nazionale di Ripresa e Resilienza* – PNRR), Italy was able to obtain the funds that the Next Generation EU had planned for it. In the PNRR, cybersecurity plays an important role, since it is considered a precondition for the proper functioning of the country's digitisation system. The text of the National Recovery and Resilience Plan can be found at https://italiadomani.gov.it/en/home.html [last cons.: 06.08.2022].

[50] This regulation can be found at https://bit.ly/3AY0Mqf [last cons.: 06.08.2022].

[51] This regulation can be found at https://bit.ly/3OjrdtA [last cons.: 06.08.2022].

[52] This regulation can be found at https://bit.ly/3B6ZMQN [last cons.: 06.08.2022].

[53] Cf. in Italian B. Carotti, *Sicurezza cibernetica e Stato-Nazione*, 5 Giorn. dir. amm. 629 ss. (2020), and A. Renzi, *La sicurezza cibernetica: lo stato dell'arte*, 4 Giorn dir. amm. 538 ss. (2021).

[54] Cf. Article No. 1 co. 2 let. a) numb. 1) Decree-Law No. 105/2019, conv. Law. No. 133/2019.

[55] Cf. Article No. 1 co. 2 let. a) numb. 2) Decree-Law No. 105/2019, conv. Law. No. 133/2019.

disruption or improper use of which harm to national security may result[56]. With respect to these two categories of actors, the legislation establishes obligations of a preventive nature, designed to avoid *ex ante* a possible cyber incident or attack[57], and notification and response obligations[58].

Coming back to ACN, it seems useful to point out that it was expressly established to protect national interests[59] in the field of cybersecurity[60], instrumentally assisting the *Presidente del Consiglio dei Ministri* (the Italian Prime Minister - for simplicity's sake, henceforth PCM)[61], who has the exclusive direction and

---

[56] Cf. Article No. 1 co. 2 let. a) numb. 2-*bis*) Decree-Law No. 105/2019, conv. Law. No. 133/2019.

[57] Including: *ex* Article No.1 co. 2 let. b) Decree-Law No. 105/2019, conv. Law. No. 133/2019, the preparation and periodic updating and communication to the competent authorities of the list of networks, information-digital systems and information services of its own relevance; *ex* Article No. 7 co. 2 DPCM July 30, 2020, No. 131, the preparation of risk analysis of individual technological assets, regarding incidents or cyberattacks on their networks or information infrastructures, also regarding dependency relationships with other networks or other digital infrastructures; *ex* Article No. 8 DPCM No. 81 of April 14, 2021, the adoption of the technical cybersecurity measures established by the competent bodies at the domestic or international level aimed at securing networks, information systems and individual technological assets their components; and *ex* Article No. 1 co. 6 let. a) Decree-Law No. 105/2019, conv. Law. No. 133/2019, the communication to the Center for National Evaluation and Certification, now established at the *Agenzia per la Cybersicurezz Nazionale*, of the intention to proceed with the purchase of procurement of goods, systems or services related to information and communication technologies that can be implemented or used on the networks or information-digital systems with which public functions or crucial public services are exercised for the State.

[58] Including notifying the Computer Security Incident Response Team (CSIRT) of incidents impacting ICT assets related to its networks or information systems or IT services.

[59] In the field of public order and safety, see *ex multis* G. Corso, *L'ordine pubblico* (1979); A. Cerri, *Ordine pubblico. Diritto costituzionale*, IV *Enc. giur.* (1990); P. Bonetti, *Ordinamento della difesa nazionale e Costituzione italiana* (2000); G. Caia, *L'ordine e la sicurezza pubblica*, in S. Cassese (dir.), *Trattato di diritto amministrativo*, Vol. 1, *Diritto amministrativo speciale*, 281 ss. (2003); T.F. Giupponi, *Le dimensioni costituzionali della sicurezza* (2010); A. Pace, *La sicurezza pubblica nella legalità costituzionale*, 1 Rivista AIC (2015); E. Chiti, *Le sfide della sicurezza e gli assetti nazionali ed europei delle forze di polizia*, 4 Dir. amm. 511 ss. (2016). Recently R. Ursi, *La sicurezza pubblica* (2022).

[60] Cf. Article No. 5 co. 1 Decree-Law No. 82/2021, conv. Law No. 109/2021.

[61] Cf. Article No. 5 co. 2 second sentence Decree-Law No. 82/2021, conv. Law No. 109/2021.

responsibility for cybersecurity policies[62]. For this reason, the functions incumbent on the ACN are numerous, so an attempt has been made to group them into a few macro-areas.

First of all, ACN is in charge of coordinating the various actors on the national territory that act in cybersecurity matters[63], also for the implementation of international strategies[64]. To this end, on behalf of Italy, it takes part in cybersecurity exercises coordinated by ENISA[65].

Secondly, ACN promotes the implementation of joint actions aimed at achieving the cybersecurity, that is essential for the digitisation process of the country[66], also through the involvement of Universities and research institutions[67].

Third, ACN is the entity entrusted with the preparation of Italy's national cybersecurity strategy[68], recently approved in May 2022[69]. Because it has the task of bringing together different instances of several stakeholders, and because it is endowed with a very high level of professionalism, ACN is responsible for advisory activities in the area of cybersecurity, updating and taking care of the national regulatory framework, also expressing non-binding opinions on legislative or regulatory initiatives in this field[70], and being able to adopt soft law and technical rules[71].

---

[62] Cf. Article No. 2 co. 1 let. a) Decree-Law No. 82/2021, conv. Law No. 109/2021.

[63] Examples include the role of CONSIP, the Ministry of Economic Development and the Intelligence System for the Security of the Republic (secret services).

[64] One example is the role of the Ministry of Foreign Affairs with regard to international cooperation on cybersecurity. Cf. Article No. 7 co. 1 let. q) Decree-Law No. 82/2021, conv. Law No. 109/2021.

[65] Cf. Article No. 7 co. 1 let. o) Decree-Law No. 82/2021, conv. Law No. 109/2021.

[66] Cf. Article No. 7 co. 1 let. a) Decree-Law No. 82/2021, conv. Law No. 109/2021.

[67] Cf. Article No. 7 co. 1 let. r) and v) Decree-Law No. 82/2021, conv. Law No. 109/2021.

[68] Cf. Article No. 7 co. 1 let. b) Decree-Law No. 82/2021, conv. Law No. 109/2021

[69] The Italian National Cyber Security Strategy 2022-2026 is available in English at https://www.acn.gov.it/ACN_EN_Strategia.pdf [last cons.: 06.08.2022]. About it see in Italian P. Mascaro, *La Strategia Nazionale Cybersecurity*, Osservatorio sullo Stato Digitale IRPA (2022).

[70] Cf. Article No. 7 co. 1 let. p) Decree-Law No. 82/2021, conv. Law No. 109/2021.

Fourthly, it is up to ACN to perform the important function of cybersecurity certification[72] established by the Cybersecurity Act, as already written in the previous paragraph.

Lastly, ACN is entrusted with supervisory and sanction tasks related to some specific interventions[73]. Aspect that highlights that this agency has more than just an advisory nature.

It was written above that the Agency has been identified as the competent national (Italian) NIS authority. This directive specifies that member states may establish at their discretion the sanctions they consider most appropriate, provided they are found to have the characteristics of effectiveness, proportionality and dissuasiveness[74]. To this purpose, Legislative Decree No. 65 of 2018, in addition to introducing on the legislative level the Italian Computer Security Incident Response Team, the so-called national CSIRT, recently hinged at the ACN, also places some obligations on private entities, in adherence to the provisions of the NIS Directive. Specifically, the Italian framework, in accordance with the European framework, obligates operators of essential services[75] and providers of digital services[76] to take «appropriate and proportionate» organizational and technical measures to avoid, cope with, and manage any risks of cyberattacks on their network or digital systems[77], as well as to minimize the effects resulting from cyber incidents that may involve the security of the network and digital systems used to provide, on the one hand, essential services[78] and, on the other hand, digital services[79]. To this goal, operators of essential services and providers of essential services must notify the Italian CSIRT «without undue delay» of any incidents that have a significant impact on the continuity of the delivery of provided essential services and digital services[80].

---

71 Cf. Article No. 7 co. 1 let. m) Decree-Law No. 82/2021, conv. Law No. 109/2021.

72 Cf. Article No. 7 co. 1 let. e) Decree-Law No. 82/2021, conv. Law No. 109/2021.

73 Cf. Article No. 7 co. 1 let. d), f), h) and i) Decree-Law No. 82/2021, conv. Law No. 109/2021.

74 Cf. Article No. 21 Direttive (EU) 2016/1148.

75 Cf. Article No. 4 co. 2 Legislative Decree No. 65/2018.

76 Cf. Article No. 3 co. 1 let. i) Legislative Decree No. 65/2018.

77 Cf. Articles No. 12 co. 1 and No. 14 co. 1 Legislative Decree No. 65/2018.

78 Cf. Article No. 12 co. 2 Legislative Decree No. 65/2018.

79 Cf. Article No. 14 co. 3 Legislative Decree No. 65/2018.

80 Cf. Articles No. 12 co. 5 and No. 14 co. 4 Legislative Decree No. 65/2018.

Compliance with these obligations is monitored by the competent (national) NIS authority[81], and in the event of violation the above private actors incur administrative fines (from €12,000 to €150,000 depending on the case), unless the act constitutes a crime[82].

ACN's sanctioning power is also referable to the National Cyber Security Perimeter (PSNC). With the obligations already described, the detailed regulations provided, in the event of their violation by those actors established by the PSNC[83], a sanction regime of a twofold nature. A regime of a criminal nature including imprisonment[84], the enforcement of which is entrusted to the Courts, and one of an administrative nature, entrusted to the ACN, which, «unless the act constitutes a crime»[85], involves the imposition of substantial administrative sanctions (from a minimum of €200,000 to a maximum of €1,800,000 depending on the specific cases).

Finally, the aforementioned Cybersecurity Act required the various European States to establish sanction provisions to be applied in the event of non-compliance with cybersecurity certification provisions[86]. As the ACN National Cybersecurity Agency has been identified as the National Cybersecurity Certification Authority, the very recent Legislative Decree No. 123 of August 3, 2022, has given the ACN some new sanctioning powers in the area of certification, consisting of monetary and accessory sanctions imposed in the event of violation of the obligations of the European cybersecurity certification framework[87].

---

[81] Cf. Article No. 20 Legislative Decree No. 65/2018.
[82] Cf. Article No. 21 Legislative Decree No. 65/2018.
[83] Cf. Article No. 1 co. 1-9 Decree-Law No. 105/2019, conv. Law No. 133/2019.
[84] For example, imprisonment is provided for those who provide untrue information, data or factual elements relevant to the preparation or updating of the *de quibus* lists or for the purposes of communications, or for the conduct of inspection and supervisory activities, or fail to communicate the aforementioned data, information or factual elements within the prescribed time limits, with the specific intent to hinder or condition the conduct of the proceedings or inspection and supervisory activities. Cf. Article No. 1 co. 11 Decree-Law No. 105/2019, conv. Law No. 133/2019.
[85] Article No. 1 co. 9 Decree-Law No. 105/2019, conv. Law No. 133/2019.
[86] Cf. Article No. 65 Regulation (EU) 2019/881.
[87] Cf. Article No. 10 Legislative Decree n. 123/2022.

These are the main tasks assigned to the ACN[88], a body that, as reconstructed, has undergone a strong centralisation of competences. To achieve the tasks entrusted to it, ACN has been granted regulatory, administrative, organisational, patrimonial, accounting and financial autonomy[89]. An aspect, the latter, that must be taken into account considering the 'classic' trend of the Italian legal framework. In recent years, in fact, new bodies have often been set up with financial invariance clauses[90], i.e. without new or additional costs for public finance. In the reality, as the literature has emphasised[91], this autonomy is highly attenuated in the face of the management-dependency relationship with the *Presidente del Consiglio dei Ministri* (PCM).

4.1. ACN and the Central Role of the *Presidente del Consiglio dei Ministri* (PCM) in Cybersecurity

It is evident, already from what has just been outlined, that there is a close relationship of direction and dependence between ACN and the *Presidente del Consiglio dei Ministri* (PCM), the Italian Prime Minister. PCM is the head of the government[92] and, as

---

[88] Additional tasks are also incumbent on the ACN. In any case, the detailed list of the various functions incumbent on the ACN is contained in Article No. 7 Decree-Law No. 82/2021, conv. Law No. 109/2021. These include, for example, the qualification function of cloud services for public administration: cf. Article No. 7 co. 1 let. m-ter) Decree-Law No. 82/2021, conv. Law No. 109/2021.

[89] Cf. Article No. 5 co. 2 second sentece Decree-Law No. 82/2021, conv. Law No. 109/2021.

[90] About this topic see in Italian F. Farri, *Le leggi con clausola di invarianza finanziaria: tra giurisprudenza contabile, giurisprudenza costituzionale e prassi del Quirinale*, 2 *L-Jus* (2021).

[91] L. Parona, *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, 6 Giorn. dir. amm. 714 (2021) who underlined the presence of «hypotheses of hetero-direction, provided for by the decree-law in favour of the President of the Council, [which] reduce the margins of autonomy actually accruing to the Agency compared to those with which, on a first analysis, it might appear to be endowed» [translation from Italian mine].

[92] It must be remembered that in the Italian constitutional system, the government is an «unequal complex organ» [translation from Italian mine], as expressly emphasised by P. Caretti, U. De Siervo, *Diritto costituzionale e pubblico* 252 (2014), as it consists of the President of the Council of Ministers, individual ministers and the Council of Ministers. Moreover, consider that the Italian Constitution states in Article 95 that «[t]he President of the Council of Ministers directs the general policy of the Government and is responsible for it. He maintains the unity of political and administrative policy, promoting and coordinating the activities of the Ministers». [translation from Italian mine]. In

already underlined above[93], has exclusive direction and responsibility for national cybersecurity policies. This dependence is indeed expressly established by its institution decree. In fact, it is the PCM who, on the one hand, determines the annual budget allocated to ACN[94] and, on the other hand, adopts the Agency's accounting regulations by his own decree, which ensures its management and accounting autonomy[95].

The aforementioned dependency relationship of ACN with the PCM can partly be explained by the central role he began to assume, as of 2007, in the field of secret services and intelligence.

In Italy, until that date, Italian secret services were composed of the Intelligence and Military Security Service (*Servizio per le informazioni e la sicurezza miliare* – SISMI) and the Intelligence and Democratic Security Service (*Servizio per le informazioni e la sicurezza democratica* – SISDE). The former was subordinate to the Minister of Defence, the latter to the Minister of the Interior. With the promulgation of Law No. 124/2007[96], the

this area see *ex multis* in Italian A. Pajno, *La presidenza del consiglio dei ministri: dal vecchio al nuovo ordinamento*, in A. Pajno, L. Torchia (eds.), *La riforma del Governo. Commento ai decreti legislativi n. 300 e n. 303/1999 sulla riorganizzazione della Presidenza del consiglio dei ministri* 35 ss. (2000); recently S. Cassese, A. Melloni, A. Pajno (eds.), *I presidenti e la presidenza del Consiglio dei ministri nell'Italia repubblicana* (2022).

[93] Cf. footnote 62.

[94] After informing the Parliamentary Committee for the Security of the Republic (COPASIR). Cf. Article No. 11 Decree-Law No. 82/2021, conv. Law No. 109/2021. However, in terms of financial autonomy, ACN is also entitled to other financial resources. Cf. Article No. 11 co. 2 lett. a)-g) Decree-Law No. 82/2021, conv. Law No. 109/2021.

[95] This adoption takes place in agreement with the Minister of Economy and Finance, on the proposal of the Director General of the Agency, after consulting COPASIR and consulting the Inter-Ministerial Committee for Cybersecurity (CIC), which will be discussed below. Cf. Article No. 11 co. 3 Decree-Law No. 82/2021, conv. Law No. 109/2021.

[96] The Law No. 124/2007 is consultable at https://bit.ly/3PIIVIf [last cons.: 06.08.2022]. This law constitutes the regulatory framework of reform of the structure and organisation of Italian intelligence and the legislation on State secrecy in Italy. On this point see in Italian *ex multis* P.L. Vigna, *La nuova disciplina dei servizi di sicurezza*, 4 Legisl. Pen. 693 ss. (2007); M. Savino, *Solo per i tuoi occhi? La riforma del sistema italiano di intelligence*, 2 Giorn. dir. amm. 121 ss. (2008); P. Bonetti, *Problemi costituzionali della legge di riforma dei servizi di informazione per la sicurezza della Repubblica*, 2 Dir. e soc. 251 ss. (2008); A. Soi, *L'intelligence italiana a sette anni dalla riforma*, 4 Quad. Cost. 918 ss. (2014); N. Gallo, T.F. Giupponi (eds.), *L'ordinamento della sicurezza. Soggetti e funzioni* (2014); recently T.F. Giupponi, *I rapporti tra sicurezza e difesa. Differenze e profili di*

secret service system began to gravitate around the figure of the Prime Minister, on whom they functionally depended[97].

Currently, the Italian secret services, whose correct definition is Intelligence System for the Security of the Republic (*Sistema di informazione per la sicurezza della Repubblica*)[98], in addition to the PCM, are composed of the Interministerial Committee for the Security of the Republic (*Comitato interministeriale per la sicurezza della Repubblica* – CISR)[99], the Delegated Authority (*Autorità delegata*)[100], the Department of Information for Security (*Dipartimento delle informazioni per la sicurezza* – DIS)[101], the Intelligence and Foreign Security Agency (*Agenzia informazioni e sicurezza esterna* – AISE)[102] and the Intelligence and Internal Security Agency (*Agenzia informazioni e sicurezza interna* – AISI)[103].

The reform of Italian intelligence, therefore, has given the PCM a role of direction and responsibility for the entire secret service sector, as underlined by the fact that, differently from the SISMI and the SISDE, the AISE and the AISI report directly to the Prime Minister and not to individual ministers.

The above-mentioned strong role of the PCM is, however, balanced by the activity of the Parliamentary Committee for the

---

convergenza, 1 Dir. Cost. 21 ss. (2022). In general on the Italian Intelligence Framework at historical and sociological plan, see G. De Lutiis, *I servizi segreti in Italia. Dal fascismo all'intelligence del XXI secolo* (2010).

97 Cf. Article No. 1 Law No. 124/2007.

98 Cf. Article No. 2 co. 1 Law No. 124/2007. It should be noted that military intelligence departments, such as the Intelligence and Security Department (*Reparto informazioni e sicurezza*), do not belong to the Intelligence System for the Security of the Republic.

99 It is composed of the Prime Minister, the Delegated Authority, the Minister of Foreign Affairs, the Minister of the Interior, the Minister of Defence, the Minister of Justice, the Minister of Economy and Finance, the Minister of Economic Development and the Minister of Ecological Transition. Cf. Article No. 5 Law No. 124/2007.

100 The Delegated Authority may be delegated, by the President of the Council of Ministers, those functions in the field of intelligence that are not exclusively attributed to it. The office of Delegated Authority may be held by an undersecretary of State or a minister without portfolio: cf. Article No. 3 Law No. 124/2007.

101 The DIS is a body of the President of the Council of Ministers and the delegated authority. It is responsible for coordinating and supervising the activities of the AISI and the AISE. Cf. Article No. 4 Law No. 124/2007.

102 Cf. Article No. 6 Law No. 124/2007.

103 Cf. Article No. 7 Law No. 124/2007.

Security of the Republic (*Comitato parlamentare per la sicurezza della Repubblica* – COPASIR), composed of ten members of Parliament (five Deputies and five Senators), which is in charge of verifying that Italian intelligence activity takes place within the limits of the Constitution and laws and in the interest of democratic institutions[104].

The centrality of the figure of the PCM in cybersecurity area also arises with regard to two other brand-new bodies: the Cybersecurity Nucleus (*Nucleo per la cybersicurezza* – NC)[105] and the Inter-Ministerial Committee for Cybersecurity (*Comitato interministeriale per la cybersicurezza* – CIC)[106].

The main function of the NC, established within ACN, is to provide support to the Prime Minister in cybersecurity matters, in relation to the prevention and preparation of possible cybersecurity crisis situations and for the activation of related alert procedures[107]. The NC is composed of the General Director of ACN (as chairman), the Military Counselor of the PCM, one representative of the DIS, one of the AISE, one of the AISI, each of the Ministers represented in the CIC and the Department of Civil Protection of the Presidency of the Council of Ministers, respectively.

Instead the CIC has the functions of advising, proposing and supervising cybersecurity policies[108]. In doing so, the CIC is responsible in particular for proposing, to the Prime Minister, the general guidelines to be pursued in the framework of national cybersecurity policies[109]; for exercising high oversight over the implementation of the national cybersecurity strategy[110]; and for promoting collaborative initiatives between institutional, national and international stakeholders and private operators interested in cybersecurity[111].

---

[104] Cf. Article No. 30 Law No. 124/2007.
[105] Cf. Article No.8 Decree-Law No. 82/2021, conv. Law No. 109/2021.
[106] Cf. Article No. 4 Decree-Law No. 82/2021, conv. Law No. 109/2021.
[107] Cf. Article No. 8 co. 1 Decree-Law No. 82/2021, conv. Law No. 109/2021. In any case, the list of individual NC functions can be found in Article No. 9 Decree-Law No. 82/2021, conv. Law No. 109/2021.
[108] Article No. 4 co. 1 Decree-Law No. 82/2021, conv. Law No. 109/2021.
[109] Article No. 4 co. 2 lett. a) Decree-Law No. 82/2021, conv. Law No. 109/2021.
[110] Article No. 4 co. 2 lett. b) Decree-Law No. 82/2021, conv. Law No. 109/2021.
[111] Article No. 4 co. 2 lett. c) Decree-Law No. 82/2021, conv. Law No. 109/2021. In relation to lett. d) of the same article, see footnote 95.

The CIC is composed of the PCM (as chairman)[112], the General Director of ACN (as secretary)[113], the Delegated Authority, the Ministers participants to the CISR[114], as well as the Minister for University and Research, the Minister of Technological Innovation and Digital Transition and the Minister of Sustainable Infrastructure and Mobility. However, emphasising once again the central role of the PCM, the rule[115] provide that the Prime Minister he may invite other members of the Council of Ministers, as well as civil and military authorities whose presence he deems necessary from time to time in relation to the issues to be addressed, to attend meetings of the Committee, without the right to vote.

From the brief analysis of the Cybersecurity Nucleus and the Inter-Ministerial Committee for Cybersecurity, the role of the PCM appears further consolidated. These two bodies are *de facto* coordinating bodies between the various actors operating in this field[116] (i.e. ACN, the Intelligence System for the Security of the Republic and Ministers), but in a servant function to the Prime Minister.

Although cybersecurity is an adjacent, but not overlapping subject to intelligence[117], it is possible to see in COPASIR the only institutionalised instrument by which Parliament and political forces of opposition can exercise (minimal) control, given that the Parliamentary Committee can request a hearing of the General Director of ACN on matters within its competence[118].

From what has been reconstructed, it emerges how, in the Italian context, the legal framework of cybersecurity has been centralized in one body, ACN. However, this process has resulted

---

112 Article No. 4 co. 3 Decree-Law No. 82/2021, conv. Law No. 109/2021.
113 Article No. 4 co. 4 Decree-Law No. 82/2021, conv. Law No. 109/2021.
114 See footnote 99.
115 Article No. 4 co. 5 Decree-Law No. 82/2021, conv. Law No. 109/2021.
116 In the field of Italian cybersecurity there are also two other bodies: the External National Assessment and Certification Centre (CVCN), set up Decree-Law. No. 105/2019, conv. Law No. 133/2019, and the Computer Security Incident Response Team - Italy, set up by Article No. 8 Legislative Decree No. 65/2018 transposing Directive (EU) 2016/1148. The institutional website is https://www.csirt.gov.it/ [last cons.: 06.08.2022]. About it see A. Renzi, *Il rafforzamento della difesa cibernetica passa per la sicurezza nazionale: il Computer security incident response team (Csirt) italiano*, Oss. Stato Digitale IRPA (2020).
117 In this sense also A. Renzi, *La sicurezza cibernetica: lo stato dell'arte*, cit. at 53.
118 Article No. 5 co. 6 Decree-Law No. 82/2021, conv. Law No. 109/2021.

in a further centralisation of competences in the hands of the PCM, the Prime Minister[119]. With all the risks and benefits that this condition brings, the words of one of USA founding fathers, Thomas Paine, still hold true: «*[s]ociety in every state is a blessing, but Government, even in its best state, is but a necessary evil; in its worst state an intolerable one*»[120].

5. Final Considerations on Participatory Cybersecurity (and Institutional Sustainability)

On the basis of the previous paragraphs, some concluding considerations can be outlined.

Some aspects emerge from the relations between the EU body in charge of cybersecurity affairs, ENISA, and the various bodies identified by the individual Member States, such as the *Agenzia per la Cybersicurezza Nazionale* in the Italian case[121].

First of all, it should be observed that the relationship between ENISA and the various national cybersecurity authorities follows the network model[122]. Specifically[123], the decentralised star

[119] As the doctrine has pointed out, the choice of legal source for approving the cybersecurity regulation reflects the centrality of the Government, as emphasised by B. Carotti, *Sicurezza cibernetica e Stato-Nazione*, cit. at 53, 639 and L. Parona, *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, cit. at 91, 718. In fact, the ACN was established by decree-law, as the legislation relating to the national security perimeter (respectively Decree-Law. No. 82/2021 and Decree-Law No. 105/2019, both later converted into Law No. 109/2021 and Law No. 133/2019). Pursuant to Article 77 of the Italian Constitution, the Government may, without delegation from Parliament, adopt provisional decrees with the force of law in extraordinary cases of necessity and urgency. Such decrees lose their effectiveness from the beginning if they are not converted into law by Parliament within sixty days of their publication. In the Italian constitutional experience, there has been a real abuse of the urgent decree-law, as the decree-law has been approved almost all the time without there being any situation of extraordinary, necessity and urgency. On this point see, in Italian, L. Imarisio, *Difetto dei presupposti per la decretazione d'urgenza e reiterazione*, in M. Dogliani (ed.), *Il libro delle leggi strapazzato e la sua manutenzione* 95 ss. (2012).

[120] M.D. Conway (coll.), *The Writings of Thomas Paine – Common sense*, Vol. I (1774-1779) 67 (1902).

[121] And this in the consciousness that such considerations are partial, having analysed only the national cybersecurity context of Italy.

[122] On the other hand, the idea that social systems, thus also including the legal system, have developed according to a network-like structure was already elaborated by Friedrich von Hayek, as reflected in F.A. Hayek, *Law, Legislation and Liberty*, in part. Voll. I e II (1973). Concerning social systems and networks,

network model[124], in which the various nodes of the network - the National Authorities of the member countries - are all connected to a central node - ENISA. The central node operates as the coordination of the network and enables the connection between the various points of the network. In fact, it is precisely through ENISA that the various authorities are interconnected. One example is the case of the joint cyber security exercises, organised by ENISA and involving national authorities. The latest exercise, Cyber Europe 2022, successfully held in June 2022, was focused on the cyber resilience strategies in the health sector[125].

As already mentioned above, the main task of ENISA is twofold. On the one hand, to establish a common level of cybersecurity across the European Union, including by actively supporting EU Member States, institutions, bodies and entities in improving cybersecurity. On the other hand, to reduce fragmentation in the European internal market for cybersecurity by promoting an EU cybersecurity policy. From this role of ENISA as an 'active promoter' of cybersecurity in the European Union, it emerges that in the field of cybersecurity the majority of competences, and the most important functions, are actually exercised by States. From the analysis of the Italian context, this aspect emerges in a palpable way, especially in view of the centrality attributed by the Prime Minister.

The network structure of this relationship thus reveals the presence of a central node endowed with different competences over and above those of the other nodes, but acting as a point of interconnection and coordination of the latter. In short: ENISA's

---

see also N. Luhmann, *Soziale Systeme. Grundriß einer allgemeinen Theorie* (1984). In relation to Luhmann's thinking applied to internal rules, see in Italian F. Fracchia, M. Occhiena, *Le norme interne: potere, organizzazione e ordinamenti. Spunti per definire un modello teorico-concettuale generale applicabile anche alle reti, ai social e all'intelligenza artificiale* (2020).

123 Indeed, it is necessary to follow the teaching Sabino Cassese, according to whom «[t]he science of law has limited itself to evoking the image of the network, which is not enough; it is also necessary to say what kind of network is involved in each case» [translation from Italian mine], S. Cassese, L. Torchia, *Diritto amministrativo. Una conversazione* 126 (2014).

124 Cf. U. Pagallo, *Teoria giuridica della complessità. Dalla "polis primitiva" di Socrate ai "mondi piccoli" dell'informatica. Un approccio evolutivo* 155 ss. (2006) in Italian, while in English A.L. Barabàsi, *Linked. The New Science of Networks* 143 ss. (2022).

125 On this topic see the ENISA official website at https://bit.ly/3OKQyNk [last cons.: 06.08.2022].

central role in the context of European cybersecurity is strengthened precisely by its task of coordinating the action of individual national authorities, which, as emerged in regard to the ACN case, are endowed with sanctioning powers - and thus with tasks further than those of a merely advisory nature. Because of the coordination of National Agencies with (also) sanctioning functions, ENISA's role appears to be reflexively strengthened, being less weak than in its early years, during which it appeared an "empty" Institution, in charge of coordinating National Agencies partly yet to be established and partly not yet endowed with incisive functions. The domestic agencies themselves, moreover, are conditioned in terms of internal operation by domestic factors. In the Italian case, for instance, the partial overlap between the intelligence and cybersecurity spheres as well as the pivotal role of the Prime Minister, the figure around whom everything rotates in this sphere.

Secondly, looking at the Italian context, it has been written about how the Italian ACN has been in establishment last year. It was not mentioned, however, that the recruitment of personnel for the Italian agency is currently still ongoing[126]. The staff is recruited with an open selection drawing mainly from the market: The overall skill level of the new ACN staff was so high that it was also praised by the hacker group *Killnet*[127].

At the current time, therefore, it is reasonable to assume that the skills of the ACN's staff are the same as those that can be found on the market. As the years go by, however, there will be the challenge of keeping the level of knowledge of the staff constantly up-to-date in an area, such as cybersecurity, where the private sector is progressing much faster than the public sector (thanks to structural advantages and other factors). And, especially in the technology sector, there is a real information gap which disadvantages the public and often results in the s.c. 'lock-in effect'.

Since ACN cannot continuously recruit new staff over the years, this situation could be solved, on the one side, by constantly upgrading staff; on the other side, by increasingly involving private cybersecurity actors. Precisely this second case could be a

[126] Cf. the ACN official website at https://www.acn.gov.it/en [last cons.: 06.08.2022].
[127] Cf. C. Bell, *Cybersecurity, the attack fails. From the hackers congratulations to Italy*, TRRA (2022).

valuable way forward. Indeed, the benefits would be considerable, particularly for the Public Administration. Moreover, there are legal principles that are useful for this purpose and on which it is possible to base this new approach (e.g. the principle of collaboration[128] and the principle of participation[129]). In this sense, the Open Government[130] strategy could be a valuable model.

In any case, the possibility of involving third parties (individuals or companies) is one of the traits that distinguish the sphere of operation of intelligence services and that of cybersecurity, as the same doctrine has highlighted[131]. And this

---

[128] About the principle of collaboration, see, *ex multis*, T. Nam, *Suggesting frameworks of citizen-sourcing via Government 2.0*, 29(1) *Government Information Quarterly* 12 ss. (2012); D. Linders, *From e-government to wegovernment: Defining a typology for citizen coproduction in the age of social media*, 29(1) *Government Information Quarterly* 446 ss. (2012); C. Cobo, *Networks for citizen consultation and citizen sourcing of expertise*, 7(3) *Contemporary Social Science* 283 ss. (2012); F. Giglioni, *Subsidiary cooperation: a new type of relationship between public and private bodies supported by the EU law*, 2 Riv. it. Dir. pubbl. comun. 485 ss. (2010); L. Hasselblad Torres, *Citizen sourcing in the public interest*, 3(1) Knowledge Management for Development Journal 134 ss. (2007).

[129] About the principle of participation, see *ex multis* A. Floridia, *The Origins of the Deliberative Turn*, in A. Bächtiger, J.S Dryzek, J. Mansbridge, M. Warren (eds.), *The Oxford Handbook of Deliberative Democracy*, Vol. I (2018); D.F. Thompson, *Deliberative Democratic Theory and Empirical Political Science*, 11(1) Annual Review of Political Science 497 ss. (2018); R. Caranta, *Civil Society Organizations and Administrative Law*, *Hamline Law Review* 39 ss. (2014); C. Coglianese, *The Transparency President? The Obama Administration and Open Government*, 22(4) Governance: An International Journal of Policy, Administration, and Institutions 529 ss. (2009); I. Shapiro, *Enough of Deliberation: Politics Is about Interests and Power*, in S. Macedo (ed.), *Deliberative Politics: Essays on Democracy and Disagreement* (1999).

[130] About the Open Government see, *ex multis*, J. von Lucke, K. Grosse, *Open Government Collaboration. Opportunities and Challenges of Open Collaborating With and Within Government*, in M. Gascò-Hernandez (eds.), *Open Government. Opportunities and Challenges for Public Governance* 189 ss. (2014); D. Lathrop, L. Ruma, *Open Government: Collaboration, Transparency, and Participation in Practice* (2010); P.G. Nixon, V.N. Koutrakou, R. Rawal (eds.), *Understanding E-Government in Europe: Issues and challenges* (2010). On this topic, in Italian see S. Rossa, *Contributo allo studio delle funzioni amministrative digitali* (2021).

[131] Cf. L. Parona, *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, cit. at 91, 718 and R. Brighi, P.G. Chiara, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, cit. at 36, 40 ss.

despite the awareness of critical profiles that in any case permeate the field of cybersecurity[132].

The welcome closer involvement of third parties in cybersecurity contrasts with the strong centralisation of this matter in the hands of the government, as is the case for instance in Italy in relation to the figure of the *Presidente del Consiglio dei Ministri*. Centralisation which, if it can be justified in view of the critical nature of cybersecurity issues and their link with the intelligence sphere, can undoubtedly be criticised in relation both to the level of parliamentary and political minority control, and to the strong political instability that characterises the alternation of governments in Italy[133]. It is clear that this contrast could also result, over time, in a downsizing of the central role of the President of the Council. And this re-dimensioning could also benefit the role of ENISA whose competences could be strengthened in the consolidation of the European *federalizing process*[134].

From what has been described in the previous paragraphs, the cybersecurity appears to be an important and crucial strategy for both the European Union and the individual Member States[135].

From this perspective, cybersecurity can be seen as a valuable tool that can implement Goal No. 16 of the United Nations Agenda 2030 for Sustainable Development[136], dedicated to promoting peaceful and inclusive societies for sustainable

---

[132] For instance, the issue of cyber protection of infrastructures that concern essential services crucial to State security.

[133] For a general overview of the duration of governments in Italy see, in Italian, L. Tentoni, *Crisi di governo? In Italia è quasi normale: in 73 anni di repubblica 6 anni in "ordinaria amministrazione"*, in Lab Parlamento (2019), in https://bit.ly/3vlpUnu [last cons.: 06.08.2022].

[134] The reference is to C.J. Friedrich, *Trends of Federalism in Theory and Practice* (1968).

[135] So crucial that part of the literature has seen cybersecurity as a public good. Cf. R. Brighi, P.G. Chiara, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, cit. at 36, 40 ss. In this sense, albeit with some distinctions from the Authors just mentioned, also M. Taddeo, *Is Cybersecurity a Public Good?*, 29 Minds & Machines 354 ss. (2019) and P. Rosenzweig, *Cybersecurity and Public Goods: The Public/Private "Partnership"*, in P. Rosenzweig, *Cyberwarfare: How Conflicts in Cyberspace are Challenging America and Changing the World* (2012).

[136] Cf. https://www.un.org/sustainabledevelopment/development-agenda/ [last cons.: 06.08.2022].

development, as well as providing universal access to justice, and building accountable and effective institutions at all levels.

A more participative cybersecurity, open to the participation and collaboration of private actors could in fact lead to «[d]evelop effective, accountable and transparent institutions at all levels»[137], as well to «[s]trengthen relevant national institutions, including through international cooperation, for building capacity at all levels, in particular in developing countries, to prevent violence and combat terrorism and crime»[138]. Opening it up to private actors would strengthen cybersecurity as it would involve the same society it is aimed at defending. And at the same time it would make citizens aware of the risks in the area of cybersecurity.

To quote a famous statement by one of the Fathers of Italian public law, Vittorio Emanuele Orlando, «[t]he law is life»[139]. And sustainable development can rightly be seen as the projection of life into the future, the «weak voice of the other»[140] that is not yet here: future generations. The legal regulation of cybersecurity, therefore, can be a concrete and effective tool to enable public institutions to prevent, fight and cooperate to counter cyberattacks aimed at destabilising the democratic balance. And this is not only for the benefit of current generations, but also for future ones.

---

[137] United Nations Agenda 2030 for Sustainable Development, goal No. 16, point 16.6.

[138] United Nations Agenda 2030 for Sustainable Development, goal No. 16, point 16.a.

[139] V.E. Orlando, *I criteri tecnici per la ricostruzione giuridica del diritto pubblico* 16 (1925).

[140] The reference is to the title of F. Fracchia, *Lo sviluppo sostenibile. La voce flebile dell'altro tra protezione dell'ambiente e tutela della specie umana* (2010). In fact, "*voce flebile dell'altro*" in English means "weak voice of the other". About this topic see *ex multis* E. Giovannini, *L'utopia sostenibile* (2018).