RIVISTA
AIC ASSOCIAZIONE ITALIANA DEI COSTITUZIONALISTI

Rivista N°: 4/2022
DATA PUBBLICAZIONE: 30/09/2022

AUTORE: Edoardo C. Raffiotta*

CYBERSECURITY REGULATION IN THE EUROPEAN UNION AND THE ISSUES OF CONSTITUTIONAL LAW **

Sommario: 1. The emergency and the evolution of the legal framework on cybersecurity. – 2. The slow and fragmentary evolution of the EU legislature on cybersecurity. – 3. The applicable EU laws on cybersecurity and the prospects for reform. – 4. The national legal framework on cybersecurity: the Italian case. – 5. The recent expansion/invasion of the supervisory powers in the name of cybersecurity. – 6. Cybersecurity versus freedom: focus on the boundaries.

1. The emergency and the evolution of the legal framework on cybersecurity

Cybersecurity is not a new issue[1], but it certainly reached a new level of relevance, especially for jurists and constitutionalists. The primary reason is that cyber-attacks are aimed at harming information, personal data and therefore the constitutional rights of businesses and private citizens[2]. It must be also observed, however, that said attacks are increasingly aimed

* Associato di diritto Costituzionale presso l'Università degli studi di Milano Bicocca.

** This article reproduces the expanded and revised text of the speech to the BeItalia 2022 Symposium, held at the School of Law of the University of California at Berkeley on June 23, 2022.

[1] Back in 2010 the Committee on National Security Systems already defined cybersecurity as "the ability to protect or defend the use of cyberspace from cyberattacks" (Committee on National Security Systems, National Information Assurance (IA) Glossary, April 2010, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf); while the U.S. Dept. of Homeland Security, National Infrastructure Protection Plan defined cybersecurity as ""[t]he prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability" (http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf, as cited in A. J. Burstein, *Amending the ECPA to enable a culture of cybersecurity research*, Harvard Journal of Law & Technology, Vol. 22, n. 1, 2008. In the EU the term "cybersecurity" appeared for the first time in a report of 2008 (see above, par. 2.) For a wider look on the different aspects of cybersecurity, see also P. Cornish, *The Oxford Handbook of Cyber Security*, Oxford University Press, 2021.

[2] For a broader perspective about the relationship between the most recent digital technology and its role in the developing of human rights see also T. E. Frosini, *Libertè, egalitè, internet*, Napoli, 2015. The debate indeed started in the U.S. literature in the mid-1950s, beginning with the 1956 Dartmouth College conference, and the Massachusetts Institute of Technology's Group on AI established in 1958 by J. McCarthy and M. Minsky. In the Italian literature it began in the late 1960s, for all see the many pioneering writings of V. Frosini, beginning with *Cibernetica diritto e società*, Milan, Edizioni di Comunità, 1968.

L'Associazione Italiana Costituzionalisti è iscritta al Registro Operatori della Comunicazione dal 9.10.2013 col n. 23897 La Rivista AIC è registrata presso il Tribunale di Roma col n. 339 del 5.8.2010 — Codice ISSN: 2039-8298 (on-line) Rivista sottoposta a referaggio — Rivista inclusa nella classe A delle Riviste scientifiche dell'Area 12 - Scienze giuridiche Direttore Responsabile: Prof. Sandro Staiano — Direttori: Prof.ssa Elisabetta Catelani, Prof. Claudio Panzera, Prof. Fabrizio Politi, Prof.ssa Antonella Sciortino.

at undermining the political stability of states, in some cases even organized unsurprisingly by other Governments, and used like a military weapon[3]. In other words, it is an issue that affects not only public safety, but also the defense of a legal system and the Nation behind it[4]. If in the past military defense concerned sea, land and air space, today cyberspace must be also taken into consideration[5].

However, the risks are even more widespread and complex. When talking about cybersecurity, it is common to distinguish between the businesses that have already suffered a cyberattack and those who have yet to be hit by one. Regrettably, this bitter consideration is starting to hold true for private citizens and public administrations as well. Therefore, in Europe the law has become an instrument to regulate the procedures and safeguards and to establish institutions that will ensure a defense and security system, hence creating the opportunity to rethink the old categories of public law and to establish new ones.

In the analysis of these recent matters however, the latest scenario in which the legal systems have to face new challenges should not be overlooked. First of all, it is important to

[3] In July 2021, the FBI and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) released a statement exposing that "Chinese state-sponsored hackers breached the networks of at least 13 oil and natural gas pipeline operators between 2011 and 2013" (https://www.cisa.gov/uscert/ncas/alerts/aa21-201a). Also in July 2021 NATO released a statement aknowledging other "national statements by Allies, such as Canada, the United Kingdom, and the United States, attributing responsibility for the Microsoft Exchange Server compromise to the People's Republic of China" (https://www.nato.int/cps/en/natohq/news_185863.htm). In August 2021, Russia targeted and blocked content on "smart voting" app created by Kremlin critic Alexei Navalny and his allies intended to organize voting against the Kremlin in next month's parliamentary elections; while the EU release on September 24, 2021, a declaration by the High Representative "on respect for the EU's democratic processes", urging Russia "to adhere to the norms of responsible state behaviour in cyberspace" (https://www.consilium.europa.eu/en/press/press-releases/2021/09/24/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-respect-for-the-eu-s-democratic-processes/). More examples can be found listed at https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. R. F. Turner theorized a precise need of establishing and enforcing reasonable standards of behavior to address cybermisconduct, perhaps by treaties or other international agreements (R. F. Turner, *Cyberdeterrence*, Harvard Law Review Forum, vol. 126:181). A partially different perspective can be found in S. T. Lawson, *Cybersecurity Discourse in the United States. Cyber-doom rethoric and beyond*, Routledge, 2021 (1st ed. Taylor and Francis, 2019), in which the Author states that the United States faces very real cybersecurity challenges that are, nonetheless, much less dramatic than what is implied in the rhetoric of the "cyber-doom" scenarios (cyberattacks against critical infrastructure resulting in catastrophic physical, social, and economic impacts). Nonethless, the A. says that "relying on cyber-doom rhetoric to frame our thinking about such threats is counterproductive", thus encouraging us to develop ways of thinking and speaking about cybersecurity "beyond cyber-doom".

[4] For a timely reflection on the relationship between security, the right to security and rule of law, see N. Zanon, *Un diritto fondamentale alla sicurezza?*, in *Diritto penale e processo*, 11, vol. 25, 2019, who remembers that "precisely in those who desire the maximum expansion of freedoms should not lack the concept that the aspiration for security, first and foremost of one's life and property, lies at the origins of the formation of the modern state as we have known it".

[5] As it is well-know, cyber-space has been designated as "a domain in which Nato will operate and defend itself as effectively as it does in the air, on land, and at sea", as recently stated by Nato Secretary General Jens Stoltenberg.

The relevance of cyberspace for the law is not a new one: for an earlier perspective see David R. Johnson & David Post, *Law and Borders — The Rise of Law in Cyberspace*, 48 Stanford Law Review, 1367, 1393-97, 1996. Back in 2010, cyber warfare had already been defined as "tomorrow's battlefield" (J. A. Ophardt, *Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield*, 9 Duke Law & Technology Review 1-28 (2010).

take into account the advancement of new technologies – for instance, artificial intelligence[6] – that are massively widespread across all businesses and the daily life of private citizens: smartphones, home appliances, self-driving vehicles are the most common examples[7].

In this context, a further substantial shift towards a general digitization of most services – including the public services, or those that are of public interest (as recently shown by the public health sector)[8] – has occurred following the COVID-19 pandemic of 2020 and the lockdown measures. These particular circumstances have forced even the most reluctant to make a not always successful digital conversion in many fields, from education to telemedicine, even in countries that were less inclined to digitization. In this respect, various statistics describe trends towards digitization that have no comparable precedent in most developed economies[9].

Evidently, this new reality has increased the opportunities for the occurrence of cyberattacks and the interest of some organizations in perpetrating cybercrimes (thus, the interest of governments in protecting their own infostructure and also the one of their citizens)[10].

The pandemic, which many countries have not yet conquered (or do not want to[11]), has been followed by the recent Russian-Ukrainian conflict which is, among other things, also a cyber conflict[12]. However, it is undeniable that, with all probability, the cyber conflict between

---

[6] See among others A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in BioLaw Journal-*Rivista di BioDiritto*, 1/2019 (in which the Author concludes by calling for a new doctrine of "precautionary constitutionalism" through which protection of fundamental rights and the rule of law should be granted within designing new technologies) and from the same Author, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, 2019.

[7] See also S. Sun Beale, P. Berris, *Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*, 16 Duke Law & Technology Review 161-204 (2018).

[8] European Parliamentary Research Service (2021), *The rise of digital health technologies during the pandemic*, Brussels.

[9] 51% of enterprises in the services sector reported disrupted business operations due to the COVID-19 outbreak, as well as in the transport and commerce and hospitality sector; while 31% in the industry sector and 26% in the construction sector (Eurofound (2021), 'COVID-19: *Could businesses have done better?*', according to which "during the first wave of the pandemic in April 2020, in almost 60% of EU companies at least some employees switched to telework. In 2019, pre-pandemic, only a quarter of these companies had employees working from home"); see also McKinsey & Company (2020), *How COVID-19 has pushed companies over the technology tipping point – and transformed business forever* , New York.

[10] As previously stated in *U.S. v. Mitra*, "Congress has the power to protect [a computer] from a local hammer blow, or from a local data packet that sends it haywire", considering every computer connected to the Internet as affecting interstate commerce and therefore protected under the CFAA (18 U.S.C. § 1030 (e)(2)(b) (2012) and I. Vasiu, L. Vasiu, *Break on Through: An Analysis of Computer Damage Cases*, *Pittsburgh Journal of Technology Law & Policy*, *14*(2), 158–201, as cited in S. Sun Beale, P. Berris, cit).

[11] See also J. Yoo, H. K. Dhillon, *Statewide Lockdowns And The Law. Hasty infringements on individual rights at a time of coronavirus*, Hoover Institution, Stanford University, 2020; and J. Yoo, *Pandemic Federalism*, National Review, 2020, also in *Who Has the Power to "Reopen" the Country?*, National Constitution Center, podcast, April 23, 2020. For an analysis of the indirect effects of the pandemic and lockdowns, e.g., on families and women, see M. D'Amico, *Una parità ambigua. Costituzione e diritti delle donne*, Raffaello Cortina Editore, 2020, who reports that during the lockdown period, complaints decreased by 50 percent (due to inability or fear) while reports to protection centers increased by 60 percent.

[12] According to the Cybersecurity and Infrastructure Security Agency "Russia's invasion of Ukraine could impact organizations… to include malicious cyber activity against the U.S. homeland, including as a response to the unprecedented economic costs imposed on Russia by the U.S. and our allies and partners" (https://www.cisa.gov/shields-up).

Russia and other countries of the Atlantic Alliance started much earlier, and in a way that was not always evident. The Cambridge Analytica case, to name the most well-known one, is perhaps the most emblematic example of how to shape the democratic consensus through the creation of fake news and deepfakes[13].

It is fundamental to take this pre-existing context into account in order to understand the evolution of the EU legislation on the matter of cybersecurity. The EU legal sources indeed predate the crucial happenings of the pandemic and the Ukrainian conflict. However, it is from the change of the prior order that the EU strategy has been relaunched, in conjunction with the new NIS Directive.

It is also important to apply the same context at a national level to better understand the incisiveness of the powers entrusted to the government that are determined by national legislation and supervise emergencies, such as the pandemic and later the Russian-Ukranian military conflict. It must be observed that the effects of new emergencies, or better of the new nature of the emergencies, impact the digital space[14] and thus prove to be less understandable to most.

Moreover, looking specifically at Italy, the powers that the law – or better, the Decree-Laws – entrusts to the Government are increasingly incisive, raising doubts about the balance between security and rights and their compatibility with the Constitution, as they often pervasively affect and constrict some areas of freedom[15].

For a broader perspective about cybercrimes and national borders see also A. Perloff-Giles, *Transnational Cyber Offenses: Overcoming Jurisdictional Challenges*, in The Yale Journal of International Law, Yale Law School, 2018; and H. H. Koh, *International Law in Cyberspace*, Harvard International Law Journal, vol. 54, 2012.

[13] See also B. Chesney, D. Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, California Law Review, n. 6, vol. 107, 2019: according to the AA., "our legal and policy architectures are not optimally designed to respond" to the rise of deep fakes and to the ways in which today's social media-oriented information environment interacts with our cognitive biases; and A. Hunt, M. Gentzkow, *Social Media and Fake News in the 2016 Election*, Journal of Economic Perspectives, 31 (2): 211-36, 2017. According to J. M. Balkin, recent calls for a solution to the problem of fake news are examples of the emergence of "new school" speech regulation, a new form of government speech regulation: a form that is "not aimed at speakers or publishers; it is aimed at digital infrastructure" (J. M. Balkin, *Old-School/New-School Speech Regulation*, 127 Harvard Law Review, 2296, 2298, 2014).

For the relationship between technology, consumption of information and its impacts on electoral economic playground – as seen in the Cambridge Analytica case – see also S. Ahmad, *Unmaking democracy*, Harvard International Review, Vol. 41, No. 2, 2020; more recently, see also E. Longo, *The Risks of Social Media Platforms for Democracy: A Call for a New Regulation*, in B. Custers, E. Fosch-Villaronga. *Law and Artificial Intelligence*, Berlin, Springer-The Asser Press, 2022.

[14] See also G. de Vergottini, *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, in Rivista AIC, 4/2019.

[15] See A. Mangia, *Emergenza, fonti fatto e fenomeni di delegificazione temporanea*, in *Rivista AIC*, 2/2021 with regard to the unexpected appearance of the dPCMs as instruments available to the government for managing crisis situations in Italy; while G. Azzariti, *Il diritto costituzionale d'eccezione*, *in Costituzionalismo.it* 1/2020 writes of "a full and lonely assumption of political responsibility by the incumbent Prime Minister in matters of fundamental citizen's rights". See also E. Raffiotta, *Sulla legittimità dei provvedimenti del Governo a contrasto dell'emergenza virale da Coronavirus*, in Biolaw Journal-*Rivista di Biodiritto* 1/2020 (more broadly about administrative powers and sources of law: E. C. Raffiotta, *Norme d'ordinanza. Contributo a una teoria delle ordinanze emergenziali come fonti normative*, Bologna, BUP, 2019; G. Morbidelli, *Delle ordinanze libere a natura normativa*, in *Dir. Amm*. 1-2/2016). That of balancing and the difficult balance between security/surveillance and rights is obviously an issue that has already appeared outside of Italy: see W. W. Keller, *Democracy Betrayed: The Rise of the Surveillance Security State*, Berkeley, CA, Counterpoint, 2017.

2. The slow and fragmentary evolution of the EU legislature on cybersecurity

The necessity of regulating the security of networks and digital applications has been clear since the beginning, when it was understood that the issue of cyber risk would have had direct effects on the information, the data and the services that these networks and applications provide and thus having direct and catastrophic effects on society and constitutional liberties.

The first acts of guidance and strategy of the cybersecurity policy have been adopted at EU level since 2000, the year in which the Communication from the European Commission on the fight against cybercrime was adopted[16]. In the first policy documents, the "security of networks" is mentioned. The EU tried to delineate a first strategy to spot the possible critical elements. At that time, the term cybersecurity was not yet used, and it would appear only in the report of 2008, suggesting a broader meaning in relation to the attention to the issue. Until that time, there was in fact talk of cybercrime and protection of personal data and critical infrastructures, but without any reference to the more comprehensive concept of cybersecurity[17].

Since then, there has been a continuous, albeit slow and fragmentary[18] evolution of the policies on cybersecurity. However, for the aforementioned reasons, it is undeniable that in the last two years it has suddenly expanded their scope, both at EU and national level, especially in Italy.

The first and more structured policy document was drafted in 2001: a Communication from the Commission of general scope on the security of networks[19], in which the outline of the NIS (Network and Information Security) Directive was established. The document describes a general overview of the cyberthreats that may fall under the NIS Directive, sorting them by nature and the degree of seriousness, for instance the unauthorized access to computers and networks or the execution of "malicious" softwares that modify or delete data. Moreover, said document also makes a reference to broad and structural risks called "disruptive attacks", which entail the interruption of the functions of infrastructure, even a critical one. They can also impact the system of an entire Country with serious damages, and not only economic ones[20].

The policy documents also highlight the security issues caused by natural events, meaning unforeseen events, including all those cases that are not caused by human action. In other words, issues that are not caused by criminal attacks: e.g., natural disasters, hardware

---

[16] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52000DC0890

[17] C. Cencetti, *Cybersecurity: Unione europea e Italia Prospettive a confronto*, in *Quaderni IAI*, 2014.

[18] According to the Italian national strategy on cybersecurity, "at the EU level, excessive fragmentation and competition among member states has, to date, been a major obstacle to the development of "made in EU" technology and the creation of large digital service delivery companies" (CAN, *Strategia nazionale di cybersicurezza 2022-2026*, https://www.acn.gov.it/ACN_Strategia.pdf).

[19] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52001DC0298

[20] See. C. Cencetti, cit., p. 23

or software failures (indeed, “threats such as environmental incidents or human errors which disrupt the network are potentially as costly as malicious attack”). Moreover, the policy documents also point out that in case of security incidents due to natural causes (floods, storms, earthquakes), it is during such events that functioning communication lines are most needed: therefore, the fundamental characteristics of networks and information systems should include availability, authentication, integrity and confidentiality[21].

Therefore, in the initial European strategy of 2001, even if there was no talk of cybersecurity yet, the related issues began to appear more critical, a realization that gave the first overview of some of the risks that in the future would become more widespread, along with the increase in digital connections and services.

The attention reserved to cybersecurity grew with the attention the EU itself paid to the process of digitization of the services, which was documented in the Lisbon strategy[22].

During this first phase, among various legislations that were set up, the institution of the European Network and Information Security Agency, better known as ENISA, took on an important role, though initially more formal than practical[23].

The Agency was established in 2004 by the EC Regulation No 460/2004, in which it is stated that the primary goal is to ensure “a high and effective level of network and information security within the Community and to develop a culture of network and information security”[24]. In contrast with other institutions, the ENISA, now called European Union Agency for Cybersecurity, had a slow start, entering a new phase with a partial revamping in 2013 with the approval of the first structured *EU Cybersecurity strategy* (February 7, 2013)[25]. The document was the result of a “joint effort”[26] by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy, and it illustrated the vision of the European Union towards a more complex and articulated EU policy on cybersecurity[27]. In this regard, said document laid the foundation of a policy that was more focused on the protection of the fundamental rights and privacy, imagining a multistakeholder governance that was democratic, efficient and linked to a shared responsibility of all the actors involved. Moreover, said document also presented the first practical instruments for an effective implementation of the goals within the subject of cybersecurity.

---

[21] As stated in the text of the Communication, “Network and information security can thus be understood as the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems”.

[22] European Commission, Europe 2005: An Information Society for All (COM (2002) 263), 28 May 2002, following which three important directives on NIS were approved in 2002: Directive 2002/21 / EC, establishing a common regulatory framework for electronic communications networks and services; Directive 2002/19 / EC, relating to access to electronic communication networks and related resources and their interconnection; and Directive 2002/20 / EC, relating to authorizations for electronic communications networks and services.

[23] See also B. Bruno, *Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali*, in «*Federalismi.it*», n. 14, 2020.

[24] EC Regulation n. 460/2004 of March10, 2004 establishing the European Network and Information Security Agency, art. 1.1.

[25] EU Regulation 526/2013 of May 21, 2013

[26] See. C. Cencetti, cit., p. 35.

[27] *Ibid*., 35-48.

Specifically, the concept of cyber resilience was introduced for the first time and the development of a policy on cyber defense and cyber capabilities was brought within the scope of the Common Security and Defense Policy (CSDP), advancing the development of a technology that would be applied and shared by the EU legal systems[28]. It is no coincidence that one of the objectives of the CSDP is the strengthening of the international security, also through the various agencies that are part of the CSDP structure (even for studying purposes)[29].

It is also important to mention the new role of international diplomacy, which would contribute to form a cohesive EU foreign policy on cyberspace, aimed to promote the fundamental values of the Union[30] (which is continuing - and indeed intensifying - today: according to a recent report by the European Commission, among the core capacities a county needs for good cybersecurity there is an emerging trend for those capacities related to international relations in cyberspace (including "the capacity to develop and act upon an understanding of how international law applies in cyberspace, norms of responsible state behaviour and confidence building measures", as well as the capacity "to engage in the international cyber diplomacy around these issues, for example in the UN Open-Ended Working Group and UN Group of Government Experts")[31].

It is undeniable however, that the most notable goal that the 2013 strategy achieved was laying the groundwork for the EU laws on cybersecurity in force today.

3. The applicable EU laws on cybersecurity and the prospects for reform

The current primary source for the EU laws on cybersecurity is the Directive 2016/1148 (also known as the "NIS Directive" - Network and Information Security), followed by the Regulation 881/2019, known as *Cybersecurity Act*. Two general sources, Directive and Regulation, dedicated to cybersecurity but with two different objectives.

Specifically, the main objective of the NIS Directive is to attain "a high common level of security of network and information systems", primarily by achieving – in each Member State – a minimum level of cybersecurity.

There are two main recipients of this particular objective. First of all, the stakeholders, divided between Operators of Essential Services established in the territory of the Union and Digital Service Providers operating in the EU. They are required to adopt technical and

---

[28] For a recent overview on the CSDP results see T. Tardy, *Does European defence really matter? Fortunes and misfortunes of the Common Security and Defence Policy*, European Security, Vol. 27, 2 (2018), Taylor and Francis, Routledge.

[29] The European Union Institute for Security Studies (EUISS) has recently set up an event on the Cybersecurity of 5G networks "to further mutual understanding of the use of 5G networks in a rapidly changing security environment, and to understand its vulnerabilities and benefits in different scenarios, and different sectors", looking to the 2030 scenarios. EUISS, Cybersecurity of 5G networks, July 5th, 2022, on https://www.iss.europa.eu/content/cybersecurity-5g-networks.

[30] As it can be remembered, the Strategy included in it the need to "ensure dialogue with international partners, including NATO, other international organizations and multinational Centres of Excellence, to ensure effective defence capabilities, identify areas for cooperation and avoid duplication of efforts" (2.3.) as well as establishing "a coherent international cyberspace policy for the European Union and promote EU core values" (2.5.).

[31] European Commission, *International Cyber Capacity Building: Global Trends And Scenarios*, 2021.

organizational measures to secure networks and IT systems; examine the potential risks to which their systems are exposed on a case-by-case basis; take appropriate measures to prevent security incidents or, at least, useful for minimizing their impact in the event of them occurring (thus ensuring continuity of service to end users); communicate to the competent authority, without undue delay, any security incident that has a significant impact on the continuity of the service[32]. Secondly, the States, which are entrusted with the development of a national strategy on cybersecurity (in Italy – as it will be better explained below – the National Cybersecurity Agency - ACN was recently established); as well as with the determination of specific financial penalties for operators failing to comply with the aforementioned obligations.

In short, the main objective, as made explicit by the EU Implementating Regulation 2018/151, is to involve all actors (public and private) in the elaboration of the European cybersecurity strategy[33] as well as – through national cooperation – reach cyber resilience throughout the territory of the Union. An approach therefore adopted to a definite protection of the single European market and individual citizens.

The Cybersecurity Act (EU Regulation 2019/881) then took a further, twofold step forward: on the one hand, the role of ENISA was strengthened, it was made permanent and given both additional resources and greater powers to support the Member States (including for the operational management of IT incidents)[34]; on the other hand, a common European framework was introduced for the cybersecurity certification for ICT, in order to ensure an adequate level of cybersecurity for ICT products, services and processes in the Union (several such schemes exist in most of the Member States – including Italy[35] – but the main issue relates to the absence, or the high difficulty, of mutual recognition of certifications between states: that is why the establishment of a common European framework is so important). Finally, the aim is to avoid the fragmentation of the internal market with regard to cybersecurity certification systems (also entrusted to through ENISA itself: it is foreseen that among other things the Agency "should regularly consult standardization organizations, in particular European ones, in developing the European systems of cybersecurity certification")[36].

However, this regulatory apparatus precedes the period of the major cyberattack crisis that arose as a result of the pandemic and the Russian-Ukrainian conflict, bringing to the foreground the lack of coordination of policies to combat cyberattacks at the level of the Member States[37], as well as the insufficiency of the range of application within the sectors

---

[32] https://www.itgovernance.eu/it-it/nis-directive-it.

[33] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0151&from=EN.

[34] See also https://www.agendadigitale.eu/sicurezza/cybersecurity-act-ecco-cosa-ci-aspetta-dopo-la-direttiva-nis/.

[35] The Higher Institute of Communications and Information Technology (ISCOM) certifies security in the field of information technology (OCSI). In the area of cybersecurity, the National Assessment and Certification Centre (CVCN) has been operational since July 1st, 2022 and is located within the Certification and Supervision Service of the National Cybersecurity Agency (ACN).

[36] See also B. Bruno, *cit*.

[37] Lorena Boix Alonso, director for digital society, trust, and cybersecurity for the European Commission's DG Connect department recently addressed the Covid-19 pandemic as a stress test for a better coordination among the EU member States' cybersecurity policies (see also L. B. Alonso, L. De Vizio, *Cybersecurity, Commissione europea: "Ecco la nostra risposta coordinata"*, in Agendadigitale.eu, 2022 (https://www.agendadigitale.eu/sicurezza/cybersecurity-verso-una-risposta-europea-quadro-delle-minacce-azioni-e-lacune-da-colmare/).

involved. In this context, an overall reform of the NIS Directive (so-called NIS 2) is underway, which, although in partial continuity with the previous one, should modify its approach, reviewing its scope of application and introducing some regulatory changes: to summarize, the new Directive will entail an update of the list of sectors and activities subject to IT security obligations[38] and will formally make operational the European Cyber Crisis Liaison Organization Network, or EU-CyCLONe, with the function of supporting the coordination and management of incidents. Specifically, this joint cyber unit aims at bringing together resources and expertise available to the EU and its Member States to effectively prevent, deter and respond to mass cyber incidents and crises[39]; and it is part of the progresses that the new scenario requires EU to make: the NIS Directive has proven its limitation, while – as exemplified by the Commission – the digital revolution of society (also intensified by the COVID-19 crisis) has "expanded the threat landscape and is bringing about new challenges, which require adapted and innovative responses", on the key assumption that today "any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the whole internal market"[40].

On May 13, the Parliament and the Council reached an agreement, which will therefore soon be subject to the approval of both.

In light of this scenario, from a public law perspective, the most notable elements characterizing the European approach are: a) the protection and promotion of the digital single market; b) the protection of individual rights; c) the direct, full involvement of all key players (both public and private, through a "hybrid formula" that obliges the former to achieve certain minimum objectives, while attempting to recognize the latter an at least partially "empowering" function). All this, in a context which - through standardization regulations[41] - aims to be almost pedagogical, necessarily implying a constant activity of public information, training and coordination.

---

[38] More specifically, the new Directive will add to the existing framework new sectors based on their criticality for the economy and society; it will include all medium and large companies in its scope; it will eliminate the distinction between operators of essential services and digital service providers; while imposing to companies "a risk management approach", stating a minimum list of basic security elements that have to be applied. Finally, it will address security of supply chains and supplier relationships, by requiring individual companies to address cybersecurity risks in it, and by carrying out thorough Member States "coordinated risk assessments…building on the successful approach taken in the context of the Commission Recommendation on Cybersecurity of 5G networks" (read more on https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union).

[39] https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3088.

[40] https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union.

[41] That is the same approach which is being adopted by the EU in others areas, such as AI regulation (as can be seen in the Proposal for a regulation of the european Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts (COM(2021)206 del 22/04/2021). For the relationship and similarities between cybersecurity – AI approaches see also G. Corasaniti, *Intelligenza artificiale e sicurezza informatica tra standards tecnologici e fattore umano*, in AI Anthology, G. Cerrina Feroni, C. Fontana, E. C. Raffiotta (a cura di), ilMulino, 2022.

4. The national legal framework on cybersecurity: the Italian case

At national level, the legal systems of the Member States can react to cyber-attacks very differently[42]: however, there is no lack of cases in which the issue has become a focal issue within the national political agenda. This is certainly the case for Italy, which has built a special institutional and regulatory apparatus, also in order to recover a general delay in competitiveness in the level of digitization of the country[43]. The transposition of the NIS Directive (through the Legislative Decree n. 65/2018) was followed - through the Decree-Law n. 105/2019, subsequently converted into law n. 133/2019 – by the establishment of a national cybersecurity Perimeter, introducing specific cybersecurity obligations (including the obligations of prior or ex post notification to the Authority) for those entities – identified by the Public Administration – who carry out an essential function or provide an essential service for the State (with two main objectives: "to ensure a high level of security of the networks, information systems and IT services of public administrations, of entities and public and private operators with headquarters in the national territory, on which the exercise of an essential function of the State depends" and "ensure the provision of an essential service for the maintenance of civil, social or economic activities, fundamental to the interests of the State and of which the malfunction, interruption and even partial or improper use would jeopardize national security")[44].

The establishment of the Perimeter was then implemented with subsequent interventions, by decree. The main interventions can be summarized as follows. The Prime Ministerial Decree (DPCM) 131/2020 established the parameters by which to identify the entities who perform essential functions for the State (therefore, falling within the national Perimeter). Individual entities are identified by the specific public administration competent for each sector (internal; defense; space; energy; etc.). The DPCM 81/2021 made a subdivision into different categories for incidents (more or less serious) having an impact on ICT assets: the classification affects the timing of communications to the CSIRT (Computer Security Incident Response Team), which the entities identified within the security Perimeter are required to carry out (obligation to notify within 1 hour for the most serious cases and 6 hours for the less serious cases); without limiting the eventuality of a voluntary notification of other incidents. The security measures required for each ICT asset must also be communicated to the Authority. The Decree of the President of the Republic (DPR) n. 54 of February 5, 2021, identified the procedures, methods and terms to be followed for the acquisition of relevant ICT

[42] See also E. Minniti, *Cyber-spazio ed intelligence: le nuove frontiere della sovranità nazionale*, in *Forum di Quaderni Costituzionali*, n. 6, 2016.

[43] The narrative of the forthcoming digitalization of Public Administration firstly began with the legislative decree n. 82/2005, following art. 10, law n. 229/2003. The relationship between technology and administration has been speculated in the doctrine before., see A. Usai, *Le prospettive di automazione delle decisioni amministrative in un sistema di teleamministrazion*e, in *Il Diritto dell'informazione e dell'informatica*, 1993, fasc. 1 p. 163 ss.

[44] Decree-Law n. 105/2019, art. 1.

assets by the entities included in the Perimeter, in addition to identifying the methods and terms within which the competent Authorities carry out verification and inspection activities. This provision was completed with the subsequent DPCM of June 15, 2021, that identified the categories of ICT assets intended to be used within the national cybersecurity Perimeter (e.g. hardware and software components that perform network functions and telecommunication services), and with the DPCM of May 18, 2022, on accreditation of testing laboratories and connections between the National Assessment and Certification Center (CVCN), accredited testing laboratories and Assessment Centers of the Ministry of the Interior and the Ministry of Defense[45].

Therefore, the entities that fall within the national Perimeter – which is very broad – are burdened by various duties and obligations. Especially when they intend to acquire supplies for their infrastructures: they must inform the public authority, which must subsequently give the authorization to proceed with the acquisition. As mentioned, these duties are not only reserved to public entities, but also private individuals who operate in sectors considered strategic or of national interest.[46]

A public authority is the main actor at the center of the supervision, support and verification activities that were described above: for Italy, it is the National Cybersecurity Agency, which from an organizational perspective is placed under the direction of the President of the Council of Ministers, the Head of the Government. The Agency has been established in June 2021 and it has the task of "promoting the implementation of common actions aimed at ensuring the security and cyber resilience necessary for the digital development of the country"[47]. The law created an institution which performs support functions for national public and private entities included in the Perimeter with the employment of technical experts. In this respect, the structure of the Agency includes the national Computer Security Incident Response Team, or "CSIRT Italia", the National Assessment and Certification Center, for the technological scrutiny of national strategic digital assets, and the National Cybersecurity Coordination Center.

At the end of May 2022, the Agency devised a National Cybersecurity Strategy for the four-year period 2022-2026 (together with a related Action Plan). Among the main priorities: a. to ensure a cyber resilience of the digital transition of the Public Administration (PA) and industry; b. anticipating the evolution of cyber threats; c. countering online disinformation within the broader context of the so-called hybrid threat (specifically regarding elections or international crises); d. cyber crises management; e. national and European digital strategic autonomy[48]. Moreover, the Strategy highlights the importance of training and the promotion of

[45] As declared by the National Cybersecurity Agency (*infra*), the last DPCM completed the regulatory framework of the National Cybersecurity Perimeter, and it is essential "to achieve the goals contained in the National Cybersecurity Strategy, aimed at raising the security level of the infrastructure supply chain on which the delivery of essential state services depends" (ACN, July 15, 2022). A further DPCM is expected to define procedures for reporting incidents impacting networks, information systems, and IT services (according to art. 1, 3, DL 105/2019).

[46] Pursuant to Legislative Decree 105/2019 and the categories provided for by the Prime Ministerial Decree of June 15, 2021, GU 198/2021.

[47] https://www.acn.gov.it.

[48] ACN, *Strategia nazionale di cybersicurezza 2022-2026*, cit.

a “cybersecurity culture”, through an alliance between the public actors, private operators, and civil society as a whole.

5. The recent expansion/invasion of the supervisory powers in the name of cybersecurity

Public intervention has become even more pervasive recently, with the expansion of the national cybersecurity Perimeter to 5G and Cloud technologies and with the applicability of the golden-power rule to them. The Decree-Law of March 21, 2022, n. 21 (so-called “Kaspersky decree”, adopted following the Russian-Ukrainian escalation) in art. 28 includes 5G among the key technologies subjected to the golden-power rule[49]. The result is an expansion of the national cybersecurity Perimeter (with the inclusion, in fact, of 5G and Cloud), while the distinction between EU and non-EU vendors is overcome: 5G is considered as an outright infrastructure of national interest, regardless of the origin of the network suppliers. Furthermore, for all telecommunications companies/operators active in the field of 5G – and through a subsequent DPCM, also for cloud technologies – which intend to acquire goods or services relating to the design, implementation, maintenance and management of the activities referred to above, an obligation of notification is introduced, which requires to communicate to the Government an annual intervention plan that the Italian Government will then have to approve (according to art.28 paragraph 4 of the Decree), reserving the right to impose further requirements or to veto. The plan must be updated every four months in the event of further and, its contents must contain among other things: the sector affected by the notification; the purchase program; description, including the technical specifications, of the goods, services and high-tech components functional to planning, implementation, maintenance and management of the activities; complete information on the contracts in progress and on the development prospects of the 5G network, meaning of the additional systems and assets. The institution of the pre-notification was also introduced, which is the communication that companies wishing to implement market operations in strategic sectors will be able to make in advance to the government in order to formally initiate a discussion in this regard; whereas the obligations set out in the Legislative Decree establishing the national Perimeter, Legislative Decree 105/2019, remain untouched (preparation and updating of the list of networks, information systems and IT services at least annually; notification of accidents impacting networks, information systems and IT services; notification in the event that the entities included in the national cybersecurity Perimeter intend to proceed with the assignment of supplies of ICT goods, systems and services intended to be used on networks, information systems and for the performance of IT services ; etc).

[49] Stating that electronic communication services with broadband based on 5G technology constitute activities of strategic importance to the system of defense and national security, also including the cloud technology.

It should also be noted that the Government reserves the right to further expand the scope of the Perimeter (Article 28 paragraph 1 of the Decree) to include “additional services, assets, relationships, activities and technologies relevant to cyber security”.

6. Cybersecurity versus freedom: focus on the boundaries

When compared with the US legal system, the European model, but especially the Italian national one, are particularly invasive. The United States operates, at the federal level, through the Cybersecurity and Infrastructure Security Agency (CISA), which is entrusted with the task of “strengthening the security, resilience, and workforce of the cyber ecosystem to protect critical services and American way of life”, also through the implementation of “binding operational directives” and “emergency directives”[50], which require action by and coordination with some federal agencies of the civilian Executive Branch. To simplify as much as possible, it can be said that - as a study by the Department of Homeland Security (DHS) and the National Association of State Chief Information Officers (NASCIO) shows - US Cyber Governance mainly focuses its activities, at national level, in six areas: Strategy and planning; Budget and acquisition; Risk identification and mitigation; Incident response; Information sharing; Workforce and education. Finally, cybersecurity is overall guaranteed through a series of “services” provided by CISA in as many specific mission areas (of which a specific Catalog is very conveniently drawn up). Recently, the Biden Administration seems to have elevated cybersecurity to the role of “critical element of the Department of Homeland Security's (DHS) mission, a top priority at all levels of government”[51].

However, what most characterizes the US approach to the issue, at least adopting a “European” perspective, is the particular balance between state action and the obligations of the private sector: in other words, a “voluntary approach” within which there is a synergy between a “light government touch”[52] and a strong empowerment of private entities, including - above all - Big Techs corporations (which, as is well known, move between cooperation with the Government and a corresponding attention not to lose part of their power, commercial and by extension decisional).

In Europe the model is very different. Regardless of whether an entity is public or private, it is assumed that the interest in cybersecurity does not lie solely with the entity that suffers or could potentially suffer a cyber attack. The interest in cybersecurity, in those areas in which there is a national interest, justifies the attention and expansion of the government powers through the government administration, which is in many cases invasive. Some brief examples to give a better idea. First of all, it must be observed that there are many private

[50] https://www.cisa.gov/cybersecurity.

[51] https://www.dhs.gov/focus. See also C. Rahill, K. Ding (edited by), *The State of Privacy under a Biden Administration: Federal Cybersecurity Legislation, Strict Regulatory Enforcement, and a New Privacy Shield with the EU*, Harvard Journal of Law and Technology digest, 2021.

[52] See also P. Howell O'Neill, *Inside the plan to fix America’s never-ending cybersecurity failures*, MIT Technology Review, 2022.

companies operating in strategic sectors or sectors of national interest. They manage confidential and often strategic information for their business activity. Sharing such information or making the purchase of certain technologies subject to the evaluation of a government agency, certainly raises questions, and not only related to the guarantee of freedom of enterprise.

Let's think, for example, that one veto using specific software or infrastructure by pointing to domestic suppliers, such as those produced by public companies. That would effectively allow a government agency to interfere to such an extent that excessive interference in the company's activities would be suspected, certainly in the name of security.

However, freedom must also be secured and guaranteed. For that matter, arguably, the same result of pursuing infrastructure security could equally be achieved with a different approach of ex-post control and accountability, providing, for example, significant liability and penalties in the case of damage resulting from cyber attacks for which the responsible party has not been adequately vigilant and compliant with the provisions of the law.

This finding, however, is even more evident in the case of the so-called golden powers which, in sectors such as Cloud and 5G, not only supervise those who intend to purchase shares or the ownership of a company operating in this sector, but also authorize the government to check the entire technological development plan of the company annually.

In short, they clearly are measures designed to avoid influences by illiberal foreign governments, but – although often determined by emergency situations[53] – they are characterized by, at the very least, a dirigiste nature, which certainly does not reflect a liberal approach. Ensuring security, including cybersecurity, always poses a problem of balancing with freedom. The focus on boundaries, however, must always be sharp as ever and must be confirmed in the application practices.

[53] It is well known that, in Schmitt's thinking, decision-making power in the state of exception is closely related to sovereignty (C. Schmitt, *Die Diktatur. Von den Anfängen des modernen Souveränitätsgedankens bis zum proletarischen Klassenkampf*, Duncker & Humblot, Berlin, 1964, 1st ed. 1921).