RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0264 • articolo sottoposto a peer review • pubblicato in anteprima il 30 gen. 2026

Lorenzo Moroni, Nasir Muftić

Democratic governance of cybersecurity in Italy and Bosnia and Herzegovina between comparisons and perspectives

From a comparative constitutional law perspective, this article aims to investigate how democratic states, such as Italy and Bosnia and Herzegovina, should exercise their constitutional function of guaranteeing cybersecurity and, consequently, protecting fundamental rights in cyberspace through democratic governance.

Cybersecurity – Constitutional Law – Democratic governance – Fundamental rights – Technological power

La governance democratica della cybersicurezza in Italia e Bosnia-Erzegovina tra comparazioni e prospettive

Secondo una prospettiva di diritto costituzionale comparato, l'articolo intende indagare il modo in cui gli Stati democratici come l'Italia e la Bosnia-Erzegovina dovrebbero esercitare la funzione costituzionale di garanzia della sicurezza informatica e, di conseguenza, tutelare i diritti fondamentali nel cyberspazio, attraverso una governance democratica.

Sicurezza informatica – Diritto costituzionale – Governance democratica – Diritti fondamentali Potere tecnologico

L. Moroni is an Assistant Professor of Constitutional and Public Law at the University of Cagliari. N. Muftić is an Assistant Professor of Civil Law at the University of Sarajevo

This paper is a joint reflection of the two Authors. They are, however, to be attributed exclusively to Lorenzo Moroni the §§ 1, 2, 3, to Nasir Muftić the § 4, and both to Lorenzo Moroni and Nasir Muftić the § 5

1. The dominance of constitutional democracies over technological power in cyberspace

The disruptive technological progress we are witnessing, with even systems capable of self-implementation through *machine learning* mechanisms becoming established on the world stage, inevitably brings with it an exponential increase in the use of such technologies, even to cause harm to public and private entities[1].

The dangers associated with the harmful use of technology grow further if we consider that by now cyberspace and its safe accessibility by users is the necessary precondition for the full enjoyment of much of fundamental rights[2]. Reflect, for example, on freedom of speech and the rights to image, personal identity, privacy and voting.

In this regard, first and foremost, the task of promoting and protecting the full enjoyment of fundamental rights even within cyberspace rests with states. Therefore, must be rejected those ideas that by adducing the territorial encroachment of cyberspace have come to predict the eclipse of state sovereignty[3], since traditional states would be "too big, too slow, and too geographically and technically limited to regulate a global citizenry's fleeting

1. This is what emerges from the most recent studies, such as the one conducted by the Italian Association for Information Security (CLUSIT), which highlights that of the 12.732 attacks that occurred between 2020 and 2024 that can be qualified as known, serious and having a particular economic and social impact (Clusit 2025, p. 46 ff.), as many as 3.541 occurred in the year 2024 alone (*Ivi*, p. 11). This is the highest number ever. As if that were not enough, just to give an idea of the increase in the phenomenon, again in the 2020-2024 time frame, 56 percent of the total attacks recorded from 2011 to the present occurred (*Ivi*, p. 12). In other words still, it went from a monthly average of 139 incidents per month in 2019 to an average of 232 in 2023 and 295 in 2024 (*Ibidem*). To these figures, which are already sufficient in themselves to give a clear and worrying picture of today's landscape, can be added additional ones that give an idea of the impact that cyber attacks produce at the economic level. In particular, taking as reference the consequences produced by the most widespread threat, namely the *data breach*, according to the latest IBM 2024, p. 6, the global average cost of damages for a breach is $4.88 million. Whereas if one takes the cybercrime phenomenon as a whole, including direct and indirect economic consequences, then the most widely shared projections, such as that of Morgan 2023, note that the global cost will reach a total of $10.5 trillion in 2025.
2. The spread of the term *cyberspace* is due to its use by Gibson 1984. A more pragmatic definition of the term is that provided by U.S. Joint Chiefs of Staff 2011, "[A] global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers". For the connection between security and the guarantee of fundamental rights, see Giupponi 2008, p. 6 ff. On the emersion of technological power in the constitutional order and its implications, see Simoncini 2022.
3. Glenn 2013, p. 171.

interactions over mercurial medium"[4]. As argued by some, in fact, behind the "apparent weakening of the regulatory capacity of public powers due to the weakening of territorial constraints"[5], in reality would be concealed the libertarian impulses of those who would like a virtual space in which freedom can unfold unencumbered by any claim to regulation by states[6]. In fact, such a claim of "maximization of freedom"[7], appears in some way a re-proposition in virtual reality of the well-known metanarrative of "spontaneous constitutions" and its "idea of freedom as coinciding with that of liberation from the public, from the state, from political power, from the constitution, in the name of the individual and the best of all possible constitutions, the invisible one spontaneously offered to us by the market"[8].

Second, not only do states have a duty to ensure cybersecurity as a precondition for the protection and promotion of the fundamental rights of their citizens in cyberspace, but in addition, being precisely *democracies*, these states, such as Italy and Bosnia and Herzegovina, have a duty to set up cybersecurity *governance* that can be said to be democratic. Indeed, as eminently pointed out by Crisafulli, the function of Constitutions, both those more strictly of the post-World War II period such as Italy's and more recent ones such as Bosnia and Herzegovina's 1995 Constitution, is to "extend the application of the democratic principle beyond the sphere of traditional political relations, strictly understood"[9]. Therefore, while it is true that the limitation of power, as McIlwain wrote long ago, still remains "the most persistent and enduring of the essential features of true constitutionalism"[10], it is equally true that such limitation must take place according to the logic of the democratic principle. In other words, none of the forms of power, whether economic, political or, as is most relevant here, technological, can escape containment and limitation by the Constitutions[11]. And in order for this to happen even while respecting the democratic principle, there must be adequate involvement and balancing not only between public and private actors, but also between representative public institutions, think of the government and parliament.

Thus, in light of what has been said so far, the usefulness of this essay stems precisely from the comparison between two democracies such as Italy and Bosnia and Herzegovina, which are different but united by the desire to see Bosnia and Herzegovina join the European Union one day. It is certainly no coincidence that Bosnia and Herzegovina has been in official negotiations to join the European Union since March 21, 2024, but, as is well known, this is only an intermediate step that may never lead to EU membership. In fact, in order to hope to see Bosnia join the EU one day, the Balkan state must meet a whole series of requirements, not least of which is the establishment of cybersecurity governance that is not only effective but also "democratic". In this regard, comparing Bosnia and Herzegovina with Italy, which is one of the member states that has achieved the highest level of implementation of European cybersecurity legislation, this essay will seek to understand, first of all, how two democracies such as Italy and Bosnia and Herzegovina are organizing cybersecurity governance. Second, we will assess whether such governance is respectful of the democratic principle, in accordance with the requirements of their respective Constitutions (Art. 1 Italian Constitution and Art. 1 Const. Bosnia and Herzegovina), as well as Article 2 of the Treaty on European Union.

4. Boyle 1997, p. 177. On the point see also Betzu 2021, p. 168.
5. *Ibidem*.
6. *Ibidem*.
7. *Ivi*, p. 169, my translation. See, also Bauman 1998, p. 23 ff.
8. Ciarlo 2002, p. 101, my translation. Along the same lines, Irti 2000, p. 299. On the subject of state sovereignty in the face of the unprecedented challenges posed by the emergence of cyberspace, see, most recently, Barozzi Reggiani 2025, p. 1 ff.
9. Crisafulli 2015, p. 253, my translation.
10. McIlwain 1990, p. 44.
11. Luciani 1996, p. 161.

2. The governance of cybersecurity in European Union

Cybersecurity, which we can define as the defense of cyberspace infrastructure (hardware and software) and its users from external threats from any public or private entity[12], requires the provision of an adequate institutional organization to deal with the challenges and threats that daily come from the digital world. However, each state alone is unlikely to be able to concretely guarantee "security of rights" in cyberspace[13], since virtual reality, unlike material reality, is not susceptible to division into boundaries[14]. Therefore, the more the network of cooperation between states in determining a common governance of cybersecurity is extended, the more it is possible to guarantee the protection of fundamental rights in the virtual dimension[15]. This is the deeper *rationale* behind the decision of the European Union and its member states to establish a common multilevel *governance* of virtual security. Therefore, even before analyzing the characteristics of the organization of cybersecurity in Italy, it is necessary to shed light on how the European Union and broadly speaking its other member states are organizing themselves to prepare adequate *cybersecurity* governance[16].

The need to ensure the security of cyberspace infrastructure and users and to coordinate state cybersecurity regulations has led the European Union to adopt numerous acts affecting cyberspace regulation[17]. Particularly crucial among

12. This is a definition resulting from a combined reading of existing Italian and European regulations. According to Art. 2, c. 1(s) of Legislative Decree No. 138 of September 4, 2024, which refers to Decree Law No. 82 of June 14, 2021, as converted by Law August 4, 2021, No. 109, cybersecurity is to be understood as "the set of activities (...) necessary to protect networks, information systems, computer services and electronic communications from cyber threats, ensuring their availability, confidentiality and integrity and guaranteeing their resilience, including for the purpose of protecting national security and the national interest in cyberspace" (Art. 1, c. 1, lett. *a*). At the European level, however, by "cybersecurity" we must mean "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats" (Art. 2, (1), EU Regulation 2019/881). Where, "network and information system", according to Art. 4, (1) of EU Regulation 2022/2555 (NIS 2) means, according to three different but complementary meanings: a) electronic communication networks; b) one or more devices that through a program perform automatic processing of digital data; c) digital data that have been the subject of the operation of digital devices, thus those transmitted, extracted, stored, etc.
13. The expression refers to the evolution of the function of state power with respect to the protection of rights. Specifically, according to the liberal tradition, it was sufficient for the state not to act except in a repressive key to the violation of rights, whereas, with the establishment of liberal democratic constitutionalism, the state is also required to act in a preventive key to positively promote the guarantee and enjoyment of personal rights. Hence, transposing this concept to the level of security, in the words of Giupponi 2023, p. 1161, the task of the state "is not so much to guarantee a purported 'right to security' of individuals as the overall 'security of rights' of citizens" (the translation is mine). On the point, with different perspectives among them, see Baratta 2001).
14. *Contra*, in favor of self-regulation of space, see Barlow 1996; Johnson–Post 1996, p. 1371 ff. In favor, on the other hand, of agreeable state regulation of cyberspace, see Goldsmith 1998, p. 1199 ff.
15. On the importance of control and cooperation tools in achieving effective cybersecurity governance, see, above all, Pietrangelo 2024, p. 13 ff.
16. On the analysis, including diachronic analysis, of European regulation in multiple areas affecting cybersecurity, see Bederna–Rajnai 2022, p. 35 ff.
17. The European acts that, more or less directly, affect cybersecurity regulation are numerous. Limiting attention to the most relevant acts not mentioned in the core text, they range from the regulation that established the European Network and Information Security Agency (EU/2004/460), through the General Data Protection Regulation (GDPR - EU Regulation 2016/679), the Cybersecurity Act (EU/2019/881 regulation), the EU 2023/2841 regulation on the high common level of cybersecurity, and on to the Artificial Intelligent Act (2024/1689 regulation) to the Cyber Resilience Act (2024/2847 regulation) and the Cyber Solidarity Act (2025/38 regulation). For more insights into the relationship between the Artificial Intelligence Act and the Cyber Resilience Act, with particular reference to the regulation of *regulatory sandboxes*, see Bagni 2023, p. 1 ff. as well as, most recently, Bagni–Seferi 2025, p. 7 ff. and contributions cited therein. For more on the relationship between

these, however, are EU Directive 2016/1148, Network and Information System (NIS 1)[18], subsequently repealed by the more recent EU Directive 2022/2555 (NIS 2), which all member states must have implemented by October 17, 2024[19].

The current NIS 2 directive[20] fulfills the task of increasing the European Union's ability to prevent and resist cyber-attacks by strengthening EU cybersecurity and reducing threats to computer and network systems of services classified as "essential" (e.g., energy, transport, health and finance) and "important" (e.g., food, manufacturing, public administration, chemical, postal, courier, etc.)[21].

Precisely with the aim of strengthening the Union Europe's cyber infrastructure, the NIS 2 directive – following in the footsteps of the NIS 1 directive – provided for a complex system of cybersecurity governance with the pre-existing *European Union Agency for Cybersecurity* (ENISA) at its center, which is assigned the tasks of assisting and advising on the development and harmonization of member states' cybersecurity policies and regulations[22]. Alongside ENISA, the NIS 2 Directive provided for the establishment of a whole series of bodies specified in Article 1, and for what is relevant here, in para. 2, lett. a, the establishment of the national cybersecurity authorities (so-called NIS national authorities) was confirmed[23]. These NIS national authorities, assisted by *Computer Security Incident Response Teams* - CSIRTs[24], perform the crucial functions of implementing and enforcing the NIS regulatory framework, as well as overseeing its proper implementation[25]. For the successful pursuit of these goals, the NIS 2 Directive provided for the assignment of important powers to the NIS national authorities, such as "on-site inspections and off-site supervision" (Art. 32, par. 2, lett. a, NIS 2), "ad hoc audits" (lett. c), "requests to access data, documents and information" (lett. f); or powers to order those concerned "to cease conduct that infringes this Directive and desist from repeating that conduct" (Art. 32, par. 4, lett. c), "to implement the recommendations provided as a result of a security audit within a reasonable deadline" (lett. f), "to make public aspects of infringements of this Directive in a specified manner" (lett. h).

The importance of the powers held by the NIS national authorities, which in democratic states are usually the responsibility of public security authorities, combined with the crucial role they play in the successful implementation of European cybersecurity strategies suggest that the NIS direc-

the Cyber Resilience Act and other Acts concerning cybersecurity see Chiara 2022, p. 255 ff. With regard, however, to case law, with particular reference to the relationship between the protection of personal data privacy and cybersecurity see, *ex plurimis*, ECJ, judgment of October 10, 2016, C-582/14, *Breyer v. Bundesrepublik Deutschland; ECJ*, Grand Chambre, judgment of December 26, 2016, C-2013/15 and C-698/15, *Tele2 Sverige AB v. Post-och telestyrelsen*; ECJ, Grand Chambre, judgment of October 6, 2020, C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs et al.*

18. Transposed by Italy through Legislative Decree No. 65 of May 18, 2018. Both NIS 1 and NIS 2 were adopted under Article 114 TFEU, "internal market hamonization". For more insights, including critical ones, on the legal basis under Article 114 TFEU, see Poli 2021, p. 69 ff. On Article 114 TFEU, De Witte 2017, p. 59, states that "it is the most powerful tool for the expansion of the EU legislative activity".
19. Currently, 14 out of 27 states have formally transposed the NIS 2 directive. Italy has transposed NIS 2 through Legislative Decree No. 138 of September 4, 2024. For more on NIS 2, see Serini 2022, p. 241 ff.
20. For more on the system envisaged by the NIS 1 directive, see, among many others, Schmitz-Berndt–Chiara 2022, p. 289 ff.
21. Notably, NIS 2 extended the scope of NIS 1, which was limited to "operators of essential services" and "providers of digital services", see Art. 1 ff., EU Directive 2016/1148. With regard to essential and important services, see Arts. 1-3 and Annexes 1 and 2, EU Directive 2022/2555 (NIS 2).
22. See Arts. 3 ff. of EU Regulation 2019/881. With regard to the regulatory context, however, Regulation EU/2019/881 proceeded to repeal Regulation EU/526/2013, which, in turn, had proceeded to repeal Regulation EC/460/2004 (and its amendments EC/1007/2008 and 580/2011) by which ENISA was established.
23. The establishment of the NIS national authorities was already provided for in Article 8 of NIS Directive 1.
24. See Art. 1(1)(a) and Art. 10 ff., EU Directive 2022/2555 (NIS 2).
25. See Arts. 1 and 8(2), EU Directive 2022/2555 (NIS 2).

tives should be applied as uniformly as possible, at least from the point of view of the establishment of the NIS national authorities[26]. But this, in fact, has not been the case.

Actually, due to the cross-cutting nature of cybersecurity policies[27] and the wide margin of discretion that each member state usually has to implement the directives, there has been heterogeneous implementation of the NIS Directive 2 within member states[28], especially in terms of how the NIS national authorities are established[29].

A first group of states decided to entrust the role of NIS national authority to multiple independent administrative authorities or technical regulatory bodies[30]. Among them, for example, Cyprus has assigned cybersecurity functions to the independent *Digital Security Authority*[31].

A second group of states, on the other hand, has assigned the role of NIS national authority to ministries or bodies dependent on them[32]. In Denmark, for example, the functions of NIS national authority have been hinged on the *Minister for Civil Protection and Emergency Planning*[33], while in Germany, pending the transposition of NIS 2, the functions remain vested in the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*), hinged on the Federal Ministry of the Interior[34].

Finally, a third group of states has decided to assign the role of NIS national authority directly to the head of government or a government agency dependent on it[35]. Consider, for example, France and Italy, whose NIS national authorities, respectively the *Agence nationale de la sécurité des systèmes d'information* and the *Agency for National Cybersecurity*, perform their functions under the influence of the French Prime Minister[36] and the Italian Prime Minister.

Faced with the multiplicity of solutions adopted by member states, the question arises as to which of the different ways of organizing governance in cybersecurity should be considered preferable. This is a question to which it is impossible to give an unambiguous answer, since much depends on the concrete functioning of each state's form of government. However, adopting the form of state as the perspective of observation, for two reasons it can be considered that in a democracy the NIS national authorities should be hinged in constitutional bodies with political representation, thus the parliament or the government.

The first reason can be traced back to the fact that NIS national authorities – as we have already seen – exercise administrative functions, such as those of inspection, audit, requesting access to data, documents and information, which traditionally have been the responsibility of the state

26. On the ability of the harmonization of cybersecurity regulation at the European level to increase the efficiency of cyber resilience, see Schmitz-Berndt–Chiara 2022, p. 307 ff. Highlighting the fragmentation of European cybersecurity regulation Eckhardt–Kotovskaia 2023, p. 150 ff.
27. They now affect almost every aspect of daily life that has an online implication, for example: buying a product in e-commerce, requesting a document online from the public administration or searching for a word on Google.
28. This obviously applies to those 14 out of 27 states that have already formally implemented the NIS 2 directive.
29. With regard to the classification into three groups, see Lauro 2021, p. 532 ff.
30. Also included in this group of member states is Cyprus.
31. Art. 30 of the Security of Networks and Information Systems (Amendment) Law of 2025, (Law 60(I)/2025) amending The Security of Networks and Information Systems Law of 2020, (Law 89(I)/2020). Pending the formal implementation of NIS 2, Luxembourg also belongs to this set, having assigned cybersecurity functions to independent authorities such as the *Institut Luxembourgeois de Régulation and the Commission de Surveillance du Secteur Financier*, depending on their areas of responsibility, on this point, see Article 3(1) and (2), A372 Loi du 28 mai 2019.
32. Included in this group of member states are Spain; Ireland; Malta; Poland; Latvia; the Netherlands; Finland; Sweden; Slovenia; Bulgaria; Greece; Croatia; Lithuania, Estonia.
33. Chapter 3, § 20, Law No. 434, Act on measures to ensure a high level of cybersecurity (NIS 2 Act).
34. See Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 40, ausgegeben zu Bonn am 29. Juni 2017, p. 1885 ff.
35. Included in this group of member states are Belgium; Slovakia; Romania; Portugal; and Austria.
36. France still needs to transpose the NIS 2 directive.

and are exercised by public security authorities directly subordinate to government ministries, such as the Ministry of the Interior, Justice or Defense[37].

The second reason is that NIS national authorities assist member states in cybersecurity *policy-making* work. Consider, for example, the establishment of the "National cybersecurity strategy" which defines the policies and related economic resources that each state adopts on cyber security. On this point, Article 7 of the NIS 2 Directive merely provides generically that such national strategies are to be adopted by "each member state" (Art. 7, par. 1). In this way, the NIS 2 Directive would seem to open up the possibility that such cybersecurity policies can be adopted as much by the government or parliament as by administrative authorities acting independently of constitutional bodies endowed with political representation, as a NIS national authority can theoretically be. But even assuming the hypothesis that the National cybersecurity strategy can be adopted only by the government or parliament, nevertheless the NIS national authorities play a crucial role in drafting these policies. The case of Italy is emblematic, where the "National cybersecurity strategy" is adopted by the Prime Minister (after consultation with the interministerial committee for cybersecurity)[38], but is prepared by the Italian NIS national authority, called the National Cybersecurity Agency (ACN)[39].

For these reasons involving the exercise of administrative functions traditionally the responsibility of states and the involvement in cybersecurity policy work, we believe that NIS national authorities should be hinged in the government or parliament. Consequently, on the other hand, it raises concerns about assigning the functions of NIS national authorities to bodies that carry out their activities independently of constitutional bodies with political representation, such as independent administrative authorities. Indeed, it is certainly true that independent administrative authorities have contributed to the evolution of governance systems in the direction of greater efficiency, including through the reevaluation of the relationship between the public and private sectors, making it possible to solve important problems in the functioning of modern democracies[40]. However, it is equally true that independent administrative authorities, by operating unbound from the circuit of democratic legitimacy (in favor, instead, of technocratic legitimacy)[41], do not prevent the risk that they may one day acquire significant autonomy in the exercise of public power in cybersecurity matters not adequately counterbalanced by full and effective democratic oversight of parliament.

3. The governance of cybersecurity in Italy

With the implementation of the NIS 2 directive by Legislative Decree No. 138 of September 4, 2024, the NIS national authorities of the member states, including Italy[42], in addition to participating in the exercise of the policy-making function – for example, by decisively assisting policymakers in the drafting of the "National cybersecurity strategy"[43] –, they are also called upon to exercise functions of traditional state competence – such as those of supervision, implementation and especially enforcement of the NIS directives[44] –. Added to this, as repeatedly mentioned, is the fact that today cyberspace represents the main context for the exercise of many of the fundamental rights, so protecting

37. See, for example, art. 32 NIS 2 directive.

38. See, art. 4, Decree Law No. 82 of 2021.

39. See, respectively, Art. 2, c. 1(b), and Art. 7, c. 1(b), L.D. No. 82/2021.

40. See, Giraudi–Righettini 2002, p. 202 ff.

41. Donati 2017, p. 2. Also on the topic of the legitimacy of independent administrative authorities, see, among many others, Amato 1997, p. 645 ff.; Pajno 1996, p. 109; Cheli 2000, p. 130; Corletto 2003, p. 114; Riviezzo 2005, p. 338, more recently, Manetti 2023, p. 782 ff.

42. For more on the state's exclusive competence in external (art. 117, c. 2, lett. d, Const.) and internal (art. 117, c. 2, lett. h, Const.) security, as well as on the qualification of security, and consequently cybersecurity, in terms of function see Moroni 2024, p. 181 ff., as well as doctrine cited therein.

43. With regard to content, see Article 9, Legislative Decree No. 138 of 2024.

44. See Articles 10 and 34 ff., Legislative Decree No. 138 of 2024. On the role of sub-state entities in achieving cybersecurity objectives, as outlined in the DDL Cybersecurity (AC1717), see Giannelli 2024, p. 15 ff.

its security no longer means only protecting the state from internal or external aggression, but also guaranteeing its citizens the exercise of fundamental rights in virtual reality.

Because of the pervasiveness that the issue of cybersecurity has, it is necessary to have forms of parliamentary oversight of the activities of NIS national authorities and, in addition, to ensure transparency of their work. This is particularly true when these authorities are hinged in the government or, even more so, when they are independent administrative authorities.

In this regard, the Italian case is particularly interesting. The functions of NIS national authority, as well as "single NIS contact point" between the national authorities and the Commission and ENISA, are assigned by Decree Law No. 82 of 2021 first and Legislative Decree No. 138 of 2024 later to the National Cybersecurity Agency (ACN)[45]. In particular, the ACN is a government intelligence agency that performs its functions under the influence of the Prime Minister[46]. In fact, the Prime Minister has high-level direction and overall responsibility for cybersecurity policies and, in addition, has the power to appoint and dismiss the Director and Deputy Director of the Agency[47]. In addition, for the effective implementation of the NIS discipline at the sectoral level, ACN and the Prime Minister's Office are also supported by 9 ministries, which, each for matters within its competence, perform the functions of NIS sector authority[48].

However, while legislator's desire to concentrate power in cybersecurity matters in the head of the Government[49] is evident, the attempt to strengthen the parliamentary function of oversight of the executive power is equally evident. Indeed, the representative body of the electoral body, in addition to having at its disposal the classic institutions of parliamentary control of the Government[50], exercises specific control functions over the activities of the Prime Minister and the National Cybersecurity Agency. In particular, the Parliamentary Committee on the Security of the Republic (so-called COPASIR) is the body through which Parliament carries out its oversight function over the policy-making activity on cybersecurity[51]. This function, in particular, is carried out by COPASIR through multiple attributions that were not changed by the more recent Legislative Decree no. 138 of 2024, such as the power to request a hearing of the President of ACN[52] and the power to express prior opinions on the adoption of regula-

45. In this regard, see in conjunction with Articles 5 and 7 (functions) of Decree-Law No. 82 of 2021, and Articles 1(2)(e) and 10 (functions) of Legislative Decree No. 138 of 2024.
46. The ACN is endowed with some margins of independence. Pursuant to Article 5, Decree-Law No. 82 of 2021, it has regulatory, administrative, property, organizational, accounting and financial autonomy, within the limits of the decree itself.
47. Art. 2, c. 1, Decree Law No. 82 of June 14, 2021, as converted by Law No. 109 of August 4, 2021. For the sake of completeness, it is necessary to point out that a Cybersecurity Core is permanently established at ACN. This is a body that performs the function of supporting the Prime Minister's Office in aspects related to prevention, preparation of crisis situations and activation of alert procedures in the field of cybersecurity, and is composed of the Director General of the ACN, who chairs it, a military adviser to the Prime Minister's Office, a representative of the Department of Security Information (DIS), a representative of the Department of Civil Protection of the Prime Minister's Office and, for the handling of classified information, also a representative of the Central Office for Secrecy (si v. Art. 8, Decree-Law No. 82 of 2021).
48. Art. 11 of Legislative Decree No. 138 of 2024. Moreover, pursuant to Article 12 below, these NIS Sector Authorities sit on the permanent table for the implementation of the NIS framework that has been established at the NCA.
49. Caramaschi 2022, p. 76 ff. On the verticalization of cybersecurity power within the Executive, see Longo 2024, p. 328.
50. Inquiries, fact-finding investigations, hearings, questions, interpellations and motions.
51. The functions of COPASIR specifically provided for with regard to the Government's cybersecurity activity are in addition to the functions useful for the conduct of parliamentary oversight that are attributed by Law No. 124 of 2007, Art. 30 ff.
52. Art. 5, c. 6, l.d. No. 82 of 2021.

tions defining: a) the organization and functioning of ACN[53]; b) the allocation of the annual sums necessary for the functioning of ACN[54]; c) the procedures for the conclusion of public contracts of ACN[55]; d) the labor relationship with the employees of ACN[56]. In addition, again with the aim of keeping Parliament informed of ACN's activities, the Prime Minister must send both Parliament and COPASIR an annual report on ACN's activities in the previous year[57].

Thus, we cannot say that in the Italian system Parliament has no form of control of the Government in exercising the policy-making function in cybersecurity. Despite this, the system envisaged in Italy still has certain criticalities.

Indeed, given the pervasiveness of cybersecurity and the transversal nature of the matters it covers, for two main reasons the role and functioning of COPASIR appears not entirely adequate to guarantee a sufficient level of transparency of the activity of controlling political direction in cybersecurity[58].

The first reason, specific to the body itself, is due to the fact that COPASIR is designed to perform its functions with a high level of confidentiality because of its task of supervising the proper conduct of the *intelligence* activity of the Intelligence System for the Security of the Republic[59]. For example, think of its composition, which is limited to only 5 deputies and 5 senators plus the two Presidents of the Chamber of Deputies and Senate[60], or the obligation of secrecy, even after the conclusion of office, to which anyone who has acquired in the performance of his or her duties information relating to COPASIR's activities is bound[61].

The second reason, a systematic one, concerns the fact that from the establishment of the NIS authority in the Prime Minister's Office and the assignment of the Government's parliamentary oversight role primarily to COPASIR, comes an excessive concentration of power at the top of the Government. For this reason, even in the field of cybersecurity can be detected the gradual shift in balance from the legislative to the executive body that doctrine has long recorded in other areas as well[62]. Indeed, the Prime Minister plays a pivotal role not only within the Security Information System and in matters of state secrecy[63], but also within COPASIR itself. For example, COPASIR must necessarily have the consent of the President of the Council in order to obtain information and copies of acts or documents to which "confidentiality" has been opposed because of the danger they may pose to the security of the Republic[64].

53. Art. 6, c. 3, l.d. No 82 of 2021.
54. Art. 11, c. 3, l.d. No. 82 of 2021.
55. Art. 11, c. 4, l.d. No. 82 of 2021.
56. Art. 12, c. 8, l.d. No 82 of 2021.
57. Art. 14, l.d. No. 82 of 2021. On this point, see also Lauro 2021, p. 541, as well as Caramaschi 2022, p. 79 ff.
58. *Ivi*, p. 542, calls the role of COPASIR "*limiting* with respect to the breadth of areas it now presides over and *limited* both in composition and in forms of publicity".
59. *Intelligence* activity must be carried out in accordance with the Constitution, the laws and the exclusive interest and for the defense of the Republic. On the composition of the Intelligence System for the Security of the Republic see Art. 2, c. 1, of Law No. 124 of 2007.
60. Art. 30, Law No. 124 of 2007.
61. Art. 36, Law No. 124 of 2007.
62. In this regard, among many, see the contributions in Siclari 2008, as well as, recently, with particular reference to sources, Cardone 2023. Still on the subject of shifting the balance in cybersecurity governance, Lauro 2021, p. 542, notes the progressive tendency to marginalize the main seats of concerned powers (e.g., Parliament) in favor of restricted and detached seats (e.g., special parliamentary commissions).
63. In particular, if already in the previous set-up outlined by Law No. 801 of 1977 the President of the Council held a pivotal role in matters of intelligence services, such a central function was further strengthened with the reform of the organization of *intelligence* activity brought about by Law No. 124 of 2007, on this point see, on all, Giupponi 2010, p. 1 ff., as well as Giupponi 2017, p. 856 ff.
64. Art. 31, cc. 7 and 8, Law. No. 124 of 2007. Further examples from which the importance of the role of the President of the Council with respect to COPASIR can be inferred, for example, from Art. 31, c. 2, l. no. 124 of

In essence, COPASIR, because of the particular secrecy of its work and the "confidentiality" with which it routinely works in close contact with the head of the Government, does not appear to be the entirely adequate body to guarantee on its own a sufficient level of transparency even outside of Parliament[65]. Instead, the Chamber of Deputies and Senate would be more appropriate bodies to ensure transparency if they were more involved. Looking to the future then, there are many interventions that the Italian legislature could implement to involve parliamentary chambers to a greater extent[66]. Consider, for example, the provision of semiannual or four-monthly public parliamentary hearings of the ACN, or the establishment of a new *ad hoc* bicameral parliamentary committee to monitor the activities of the Government, whose greater representativeness of composition and publicity of its work would ensure adequate knowledge of the decisions taken on cybersecurity. It should not be forgotten, in fact, that "the apparatus of democracy has transparency as its rule, and secrecy is an exception"[67]. And this is all the more true for security in cyberspace, which now intersects all fields of daily life.

4. The governance of cybersecurity in Bosnia and Herzegovina

In the age of digital interdependence, cybersecurity has become not only a technical necessity but a fundamental element of state sovereignty, economic resilience, and protection of fundamental rights. This has become a truism in the 21 century Europe, which states as well as the EU have legislated and adopted policies in this matter. Bosnia and Herzegovina (BiH), however, presents an instructive case where constitutional complexity, institutional fragmentation, and weak governance have left the country exposed to mounting cybersecurity threats without a coherent or effective national response.

The Constitution of Bosnia and Herzegovina, annexed to the Dayton Peace Agreement of 1995 which ended the war, provides no explicit mention of cybersecurity. Yet the issue implicates multiple constitutional provisions. The preamble of the state Constitution proclaims that Bosniacs, Croats, and Serbs, as constituent peoples (along with Others), and citizens of Bosnia and Herzegovina are "committed to the sovereignty, territorial integrity, and political independence of Bosnia and Herzegovina in accordance with international law". The institutions on the state level[68], according to Article III(1), are responsible for matters of foreign policy, international trade, customs, defense, and general security-areas inherently tied to cybersecurity in the digital era. However, the country's constitutional arrangement is highly decentralized and labeled as "sui generis" by the state's Constitutional

2007, under which it is necessary for COPASIR to obtain the consent of the President of the Council in order to hear an employee of the Security Intelligence System, or from Art. 31, cc. 14 and 15, l. No. 124 of 2007, which stipulates that COPASIR may order access and inspections to the offices of the Security Information System only once prior notice has been given to the President of the Council, who may defer their execution in case of danger of interference with ongoing operations.

65. Moreover, there are not a few obstacles to the disclosure of secrecy in Parliament and, in addition, it is not so easy to assert the political and legal responsibility of the Government. On this point, see Bifulco 2017, p. 1115 ff.; Luciani 2013, p. 22 ff.

66. On the level of instruments of parliamentary control, Lauro 2021, p. 542, proposes the holding of annual sessions of effective control and discussion on defense and cybersecurity issues, which, therefore, go beyond "the mere acknowledgement of the Reports transmitted by the competent instances".

67. Barile 1987, p. 29; Bobbio 1991, pp. 106 and 88; Anzon 1976, p. 1761; Bifulco 2017, p. 1101.

68. The state institutions refer to the institutions at the level of the state government and not lower levels. Bosnia and Herzegovina has a complex governmental structure, It consists of the state-level government, the two entities (Federation of Bosnia and Herzegovina and Republika Srpska) and Brcko District. Moreover, the entities are asymetrical as Federation of Bosnia and Herzegovina consists of 10 cantons, while Republika Srpska fails to replicate any lower-level construction. Each of the levels of government mentioned here have their own legislature, executive and judiciary, except for cantons which judiciary is regulated mostly at the level of Federation of Bosnia and Herzegovina.

court[69]. Bosnia and Herzegovina consists of two entities – the Federation of BiH and the Republika Srpska (RS) – alongside the self-governing Brčko District. Each level of government possesses its own legislative and executive apparatus as well as the judiciary.[70] This division of powers creates legal ambiguity over which institution is competent to develop and implement cybersecurity policies. The Constitution is explicit as it suggests that the powers not explicitly assigned to the state level belong to the lower levels of government.[71] The lower levels of government may agree that the state level may assume their powers[72]. Although the matter of defense was not designated as a power of the state, the entities agreed to empower it in this matter.[73] Moreover, assignment of powers is influenced by an additional player – the Office of High Representative (OHR), an international body tasked with supervising the civilian implementation of the Dayton Peace Agreement.[74] In practice, this role is filled by a foreign diplomat or politician who holds extensive powers.[75] The most significant authority of the OHR stems from the so-called "Bonn Powers," granted in December 1997 by the Peace Implementation Council[76]. These powers enable the OHR to remove public officials who breach the obligations of the Dayton Agreement, as well as to impose laws and enact binding measures necessary to secure the enforcement of the General Framework Agreement for Peace. Since then, the OHR has had the unilateral ability to amend entity constitutions, pass legislation, and dismiss officials. The extent to which these powers have been exercised has varied over time, depending both on the individual serving as High Representative and the prevailing dynamics within the Peace Implementation Council. For example, Paddy Ashdown, one of the former High Representatives, imposed 104 laws in his first year in office between May 2002 and May 2003[77].

Bosnia and Herzegovina's political system is designed with numerous mechanisms that allow both the entities and representatives of constituent peoples to block any government decision they perceive as contrary to their interests. Rather than being citizen-centered, the system is built on a power-sharing model between the three constitu-

69. Constitutional Court of Bosnia and Herzegovina, decision number U9/ 58-III, 30. 06. i 01. 07. 2000.

70. Harun 2017, pp. 14 ff.

71. The Bosnia and Herzegovina Constitution Article III 3 stipulates: "All governmental functions and powers not expressly assigned in this Constitution to the institutions of Bosnia and Herzegovina shall be those of the Entities".

72. The Bosnia and Herzegovina Constitution Article III 5 stipulates: "Bosnia and Herzegovina shall assume responsibility for such other matters as are agreed by the Entities; are provided for in Annexes 5 through 8 to the General Framework Agreement; or are necessary to preserve the sovereignty, territorial integrity, political independence, and international personality of Bosnia and Herzegovina, in accordance with the division of responsibilities between the institutions of Bosnia and Herzegovina. Additional institutions may be established as necessary to carry out such responsibilities".

73. Harun 2017, pp. 14 ff.

74. The Dayton Peace Agreement defines the Office of High Representative. Its central part, the General Framework Agreement has eleven Annexes. Annex 10 (the Agreement on Civilian Implementation) defines the mandate of the High Representative as it follows: "the designation of a High Representative, to be appointed consistent with relevant United Nations Security Council resolutions, to facilitate the Parties' own efforts and to mobilize and, as appropriate, coordinate the activities of the organizations and agencies involved in the civilian aspects of the peace settlement by carrying out, as entrusted by a U.N. Security Council resolution, the tasks set out below". A significant development occurred in 1997, when the Peace Implementation Council (PIC) has endowed the OHR with a power to make binding decisions. The Bonn Powers grant the High Representative in Bosnia and Herzegovina broad authority to impose laws, remove elected and appointed officials, and ensure implementation of the Dayton Peace Agreement. These powers effectively allow the OHR to override domestic institutions in order to maintain peace and stability.

75. The list is available at the Office of the High Representative website.

76. *Ivi*.

77. Zvijerac 2021.

tionally recognized constituent peoples – Bosniaks, Croats, and Serbs – and the two entities[78]. Each of these groups holds guaranteed representation in legislative bodies and, in practice, is also assured positions within the executive and judicial branches. Additionally, with the exception of Republika Srpska, governments can be entirely paralyzed if the majority of representatives in the upper chamber of the legislature oppose necessary decisions[79]. This has led to prolonged institutional gridlock; for example, both the state-level government and the government of the Federation of Bosnia and Herzegovina have been effectively blocked for four years, rendering the results of past elections unenforceable. Further obstruction is possible through the executive branch, which can delay or refuse judicial appointments – such as appointments to the Constitutional Court. Compounding these structural dysfunctions, the constitutional framework itself infringes upon fundamental human rights. The European Court of Human Rights has repeatedly found that the political system discriminates against individuals who do not belong to one of the three constituent peoples, denying them the right to stand for election or to hold high public office. This was established in landmark cases of Sejdić and Finci v. Bosnia and Herzegovina[80], Zornić v. Bosnia and Herzegovina[81], Šlaku v. Bosnia and Herzegovina[82], and Pilav v. Bosnia and Herzegovina[83]. Despite these rulings, the country has failed to implement the required changes due to persistent political deadlock and the inability to reach consensus on constitutional reform.

The state-level institutions, such as the Ministry of Security of Bosnia and Herzegovina, claim constitutional competence to address issues of national security, including cyber threats[84]. Currently, there are several laws on the state level which concern cybersecurity matter, such as the laws governing electronic signature, electronic transactions, and cybercrimes and criminal procedure[85]. The state already exercises powers in this domain without a proper cybersecurity framework. Therefore, the ongoing standstill has resulted in a lack of coherent cybersecurity governance at the national level. On the other hand, the exact cybersecurity framework to be adopted should be relatively predictable. As a striving member state of the EU, Bosnia and Herzegovina entered into a Stabilisation and Association Agreement which requires it to adapt its law to the EU acquis and to establish a free-trade zone with the European Union, as well as to refrain from passing laws which are contrary to the acquis[86].

At present, BiH does not have an adopted national cybersecurity strategy. Efforts to draft such a strategy – led by the Ministry of Security with the technical support of the Organization for Security and Co-operation in Europe (OSCE) – have stalled due to political disagreement over the state-level competencies in this domain. Republika Srpska has instead developed its own cybersecurity policies, which remain separate from national efforts, thus exacerbating the legal and institutional divide[87]. It adopted the Law on Information Security in 2011. The law addressed data protection and established institutional mechanisms responsible for

78. Tahir–Muftić 2023.

79. The constitutional structure of the country can be described as consonciation as it allow ethnic groups vast veto powers. See more at Merdzanovic 2016.

80. *Sejdic and Finci v. Bosnia and Herzegovina* (27996/06 and 34836/06), European Court of Human Rights.

81. *Zornic v. Bosnia and Herzegovina* (3681/06), European Court of Human Rights.

82. *Slaku v. Bosnia and Herzegovina* (56666/12), European Court of Human Rights.

83. *Pilav v. Bosnia and Herzegovina* (41939/07), European Court of Human Rights.

84. See: *Strategy for establishment of CERT* published at the website of the Ministry of Security.

85. Law on Electronic Signature of BiH, Law on Electronic Legal and Business Transactions of BiH, Law on Prevention of Money Laundering and Financing of Terrorism in BiH, Criminal Code of BiH (parts which deal with copyright abuse), then Law on Protection of Copyright Abuse Acts, then Law on Protection of Criminal Offenses of Criminal Procedure of BiH, Law on Protection of Confidential Data of BiH, and Law on Communications of BiH.

86. Stabilisation and Association Agreement.

87. See the Government of Republik of Srpska website.

the development, implementation, and oversight of information security policies. One of the outcomes of this legal framework was the creation of the Computer Emergency Response Team of the Republic of Srpska (CERT-RS), which was designated as the entity-level CERT and became fully operational in 2015[88]. Building on this foundation, the Republic of Srpska adopted the Law on the Safety of Critical Infrastructures in 2019 and subsequently introduced the Strategy for the Fight against Cybercrime for the period 2019–2023, further expanding its normative and strategic approach to cybersecurity. The absence of a functional national Computer Emergency Response Team (CERT) further exemplifies this governance paralysis. Although the state-level authorities proposed the establishment of BiH-CERT as early as 2011, political blockages have prevented its creation. Republika Srpska maintains its own CERT operating independently from any state-level coordination mechanism. The Federation of BiH lacks an equivalent body, but it attempted to pass the equivalent law on information security in this entity in 2022[89]. The attempt was unsuccessful, rending both level of Federation BiH and the state level deregulated. There is one exception on the state level – the Ministry of Defense of Bosnia and Herzegovina, which has its own policies in this matter. To sum the current state, we can cite the EU Commission's words in the Report for Bosnia and Herzegovina for 2023: "Bosnia and Herzegovina does not have a comprehensive legislative framework on the security of networks and information systems (a law on information security is in place only in the Republika Srpska entity), and made no progress in adopting a country-wide strategy. Moreover, the country made no progress in designating a country-wide single point of contact responsible for coordination and cross-border cooperation. Bosnia and Herzegovina needs to establish a network of computer security incident response teams (CSIRT) to facilitate strategic cooperation and the exchange of information; a CSIRT is operational only at the Ministry of Defence and in the Republika Srpska entity."[90]. In practice, it means that cybersecurity incidents are often handled in an ad hoc fashion by law enforcement bodies, with limited technical capability and no unified strategic oversight.

The consequences of this fragmented approach are profound. A combination of outdated systems, weak institutional capacity, and a low level of digital literacy has created fertile ground for cybercrime, disinformation, and digital espionage. The Global Cybersecurity Index ranks BiH alarmingly low, and research conducted by Euronews has highlighted that the country faces the highest exposure to cybersecurity threats in Europe. In the absence of a coherent defense, both public institutions and private citizens remain highly vulnerable to phishing attacks, ransomware, identity theft, and other forms of cyber intrusion. The lack of a comprehensive cybersecurity strategy not only leaves the country exposed to external threats but also undermines trust in digital services, e-commerce, and e-government key drivers of economic modernization.

The gridlock has seemed to be starting to get unlocked a couple of years ago. Cyberattacks on BiH institutions[91] have spurred action. In May 2023, the Council of Ministers approved changes to the Ministry of Security's internal organization, enabling the creation of a CERT. This step could have marked the beginning of a coordinated response to cyber threats, aiding both the fight against cyberattacks and alignment with EU cybersecurity standards. The Ministry of Security planned to recruit CERT staff, develop a comprehensive operational plan, and join international CERT networks to share threat intelligence and best practices[92]. However, two years forwards, there seems to be no substantial progress. In fact, to discuss the issue of democratic governance requires a willingness to govern cybersecurity on the national level first, but so far it seems that the increased exposure of BiH institutions and citizens fails to change it.

88. The CSIRT RS is also part of the CSIRT system known as "Western Balkans".

89. See the FBIH Government website from 2022 post.

90. EU Commission, *Bosnia and Herzegovina 2023 Report*, SWD(2023) 691.

91. Available at: radiosarajevo.ba website.

92. Report of the Council of Ministers for 2023.

5. From comparison to perspective: towards democratic governance of cybersecurity in Bosnia and Herzegovina

A comparison between the Italian and Bosnian legal systems in the field of cybersecurity reveals a picture of considerable systemic complexity, marked by fundamental structural differences that require Bosnia and Herzegovina (BiH) to undertake immediate reform and adaptation in order to aspire to future integration into the European Union.

Italy, in fact, although with significant margin for improvement in terms of cybersecurity governance, remains one of the very few countries in the world to have obtained the maximum score from the International Telecommunication Union's *Global Cybersecurity Index for 2024*, unlike Bosnia and Herzegovina, which, on the contrary, is the European country with the lowest score.

From the point of view of cybersecurity governance, the study shows that there is no doubt that Italy, unlike Bosnia, has benefited from its membership of the European Union for at least two reasons. The first is that the EU, having moved early to outline the essential elements of cybersecurity governance, has substantially reduced the impact of internal political instability on the process of establishing cybersecurity governance. In fact, from a technical and political point of view, it is much easier to prepare internal legislation implementing EU directives, such as NIS 1 and 2, than draft laws that provide for a complicated system of inter-state management and cooperation on cybersecurity from the beginning. This, combined with the prescriptive force of EU directives and the sanctions mechanisms for non-compliant states, has led almost all European states, including Italy, to achieve a high degree of implementation of NIS 1 and 2. The second reason why Italy, unlike Bosnia, has benefited greatly from its membership of the European Union is that cybersecurity governance is characterized by profound and essential elements of homogeneity among European states, which therefore guarantees a very high level of cooperation within the European space. Focusing solely on institutional bodies, for example, all European states are required to adhere to the complex European cybersecurity system, which is centered on European ENISA and the national NIS authorities assisted by CSIRT emergency response units. In short, this is a system that has profound elements of homogeneity, thanks to which it has been possible to create an integrated system to combat threats from the virtual world that involves all 27 member states in a synergistic manner.

Clearly, despite these positive elements, there are some areas that need to be worked on to improve the system. As already discussed, apart from some differences in the speed of transposition of the NIS 2 Directive – which, however, is not a cause for excessive concern – it would certainly have been desirable to have a more uniform implementation with regard to the attribution of the role of national NIS authority to representative bodies, such as the government or parliament, rather than to independent administrative authorities, as was the case in Cyprus, for example.

The situation in Bosnia and Herzegovina today is quite different. In stark contrast to Italy, the fact that Bosnia and Herzegovina does not belong to a supranational organization such as the European Union has meant that the numerous problems with the effectiveness of the government's organization in Bosnia have been reflected in the governance of cybersecurity. As noted above, the combination of factors attributable to extreme constitutional complexity, institutional fragmentation, and weak government effectiveness has meant that Bosnia and Herzegovina still does not have a common cybersecurity system between the Federation of Bosnia and Herzegovina and the Republika Srpska capable of dealing with the growing threats from the digital world. As a result, the burden of developing a policy to combat cybercrime falls entirely on the state level, where the Federation of Bosnia and Herzegovina has not yet managed to adopt a cybersecurity strategy due to frequent political disagreements. Political agreement, on the other hand, has been reached at the state level in Republika Srpska, since it approved a cybersecurity strategy in 2019 and has had a Computer Emergency Response Team of the Republic of Srpska (CERT-RS) since 2015. However, the usefulness of all these measures is now inevitably compromised by the fact that all the measures adopted to combat cybersecurity are limited in scope to Republika Srpska alone, leaving most of Bosnia and Herzegovina without effective protection against cyber threats. Moreover, such approach remains futile as there

is a lack of a necessary cybersecurity framework on the state level although all levels of government have interest to have a state-level framework due to their own security.

Faced with such a fragmented landscape of Bosnian cybersecurity governance, which clearly has more shadows than lights, perhaps a glimmer of hope can be found in the very fact that a cybersecurity strategy model and a CSIRT approach at least exist at the entity level in Republika Srpska and, therefore, this could serve as a starting point for BiH to then orient its entire governance towards the provisions of the European NIS 2 Directive. This is, of course, only a glimmer of hope, but it may be worth placing some hope in it, even if its feasibility seems rather remote at present, as it would require close cooperation between the actors to establish a state-level framework.

Shifting the focus from the organization of cybersecurity governance to the democratic nature of this governance, once again the comparison confirms both positive and negative aspects on both the Italian and BiH sides.

As far as Italy is concerned, it has been noted that entrusting the role of national NIS authority to the ACN is certainly a reasonable choice. This body is technically competent and is based within the Presidency of the Council of Ministers, meaning that it is subject to the control of a politically representative body. Despite these positive elements, however, it has been argued that some critical issues remain regarding the entrusting of the role of parliamentary control mainly to COPASIR, since the strict confidentiality with which it works closely with the Prime Minister, combined with the rule of secrecy that characterizes its work, risks not only excessively centralizing cybersecurity functions at the top of the government, but also failing to ensure a sufficient level of transparency outside Parliament.

As regards Bosnia and Herzegovina, it is clear that the assessment of democracy cannot be made on the basis of state governance, but only partly, on the basis of that of the entity of Republika Srpska, because it is the only one that exists and could therefore represent a first model of approximation to the governance imposed by the NIS 2 Directive. In this regard, the Republic's decision to establish the CSIRT-RS within the Ministry of Scientific and Technological Development and Higher Education, rather than, for example, within an independent administrative authority or a private company, is understandable and technically agreeable[93]. This choice resembles the one taken by Italy with regard to the ACN and, therefore, the same concerns that apply to Italy also apply to Republika Srpska, namely the danger of excessive centralization of cybersecurity governance in the executive branch and the need to ensure not only parliamentary oversight of the executive, but also adequate transparency of cybersecurity activities.

Looking to the future, while the measures to improve the structure and democratic nature of cybersecurity governance appear to be well defined, the situation is different in Bosnia and Herzegovina.

We have already seen that, in Italy, a measure that would improve both the structure and the democratic nature of cybersecurity governance would be, for example, the replacement of parliamentary control of digital security policies mainly made by COPASIR, with the provision of semi-annual or quarterly public parliamentary hearings of the ACN, or directly the establishment of a new *ad hoc* bicameral parliamentary commission to monitor the activities of the government, whose greater representativeness in terms of composition and publicity of its work would ensure adequate knowledge of the decisions taken on cybersecurity.

With regard to Bosnia and Herzegovina, on the other hand, rather than targeted interventions, it is necessary to reflect on a real path towards the establishment of cybersecurity governance, whose structure and democratic nature reflect the provisions contained in the European NIS 2 Directive, also taking inspiration from existing models such as the Italian one.

First of all, in order to bridge the gap between the structure and democratic nature of BiH cybersecurity governance and that of Italy and other EU members, it is necessary to first establish a BiH cybersecurity body, along the lines of the Italian ACN, which will be entrusted with a series of tasks, including the essential technical assistance in the adoption of a National Cybersecurity Strategy that provides for the inclusion and cooperation be-

93. Law on Republic Administration ("Official Gazette of the Republic of Srpska", No. 115/18).

tween BiH, Republika Srpska, and the Brčko District. Secondly, again in line with the provisions of Italy and the European NIS 2 Directive, the Bosnian cybersecurity body must be supported by a State-Level CERT to combat cybersecurity threats, which must also include all state and autonomous entities within Bosnia and Herzegovina. In this regard, it should be emphasized that governance at the state level cannot be achieved as long as there is a lack of consensus of Republika Srpska, Federation of BiH and the Brcko District. This is a necessary step to achieve a unified and synergistic approach. Thirdly, in order to ensure the right level of democracy and transparency in the system thus envisaged, the BiH Parliament will need to be equipped with a whole range of tools to monitor the work of the BiH cybersecurity body and the state CSIRT. In this regard, consideration should be given to setting up an ad hoc parliamentary committee for BiH digital security, accompanied by reporting obligations at set intervals. Finally, it is essential that institutional activities in the field of cybersecurity are not limited to the mere preparation and implementation of regulatory, organizational, and technological tools for the protection of digital infrastructure, but are simultaneously integrated with adequate and systematic dissemination and education of the population, which is crucial for the overall effectiveness of public policies in this area.

In conclusion, the path that Bosnia and Herzegovina must take to adapt its structure and increase the democratic nature of its cybersecurity governance is long and complex, but at the same time essential. Its success is not only a necessary condition for legitimately aspiring to join the European Union in the future, but also an essential prerequisite for consolidating effective forms of cooperation with other democratic states. In the current global context, the protection of fundamental rights can no longer be guaranteed solely within national borders: it is only through an extensive and shared cybersecurity system, transcending the territorial boundaries of Italy, Bosnia and Herzegovina, and even the European Union, that it becomes concretely possible to ensure constitutional control of technological power, as well as the effective protection and full enjoyment of fundamental constitutional rights within the digital dimension.

References

G. Amato (1997), *Autorità semi-indipendenti e autorità di garanzia*, in "Rivista trimestrale di diritto pubblico", 1997

A. Anzon (1976), *Segreto di Stato e Costituzione*, in "Giurisprudenza costituzionale", 1976

F. Bagni (2023), *The Regulatory Sandbox and the Cybersecurity Challange: from the Artificial Intelligence Act to the Cyber Resilience Act*, in "Rivista italiana di informatica e diritto", 2023, n. 2

F. Bagni, F. Seferi (2025), *Regulatory Sandboxes for AI and Cybersecurity. Questions and answers for stakeholders*, 2025

A. Baratta (2001), *Diritto alla sicurezza o sicurezza dei diritti?*, in M. Palma, S. Anastasia (eds.), "La bilancia e la misura", Franco Angeli, 2001

P. Barile (1987), *Democrazia e segreto*, in "Quaderni costituzionali", 1987, n. 1

J.P. Barlow (1996), *A Declaration of the Independence of Cyberspace*, 1996

G. Barozzi Reggiani (2025), *La* race for the cyberspace *degli Stati e il tema della cybersicurezza: tra sovranità e modelli di governance*, in "Rivista italiana di informatica e diritto", 2025, n. 2

Z. Bauman (1998), *Globalization. The Human Consequences*, Columbia University Press, 1998

Z. Bederna, Z. Rajnai (2022), *Analysis of the cybersecurity ecosystem in the European Union,* in "International Cybersecurity Law Review", 2022, n. 2

M. Betzu (2021), *Poteri pubblici e poteri private nel mondo digitale*, in "Rivista Gruppo di Pisa", 2021, n. 2

R. Bifulco (2017), *Segreto e potere politico*, in "Enciclopedia del diritto. Annali X", Giuffrè, 2017

N. Bobbio (1991), *La democrazia e il potere invisibile*, in N. Bobbio, "Il futuro della democrazia", Einaudi, 1991

J. Boyle (1997), *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, in "University of Cincinnati Law Review", vol. 66, 1997

O. Caramaschi (2022), *La cybersicurezza nazionale ai tempi della guerra (cibernetica): il ruolo degli organi parlamentari*, in "Osservatorio costituzionale", 2022, n. 4

A. Cardone (2023), *Sistema delle fonti e forma di governo. La produzione normativa della Repubblica tra modello costituzionale, trasformazioni e riforme (1948-2023)*, il Mulino, 2023

E. Cheli (2000), *Le autorità amministrative indipendenti nella forma di governo*, in "Associazione per gli studi e le ricerche parlamentari", vol. 11, Giappichelli, 2000

P.G. Chiara (2022), *The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. An introduction*, in "International Cybersecurity Law Review", 2022, n. 3

P. Ciarlo (2002), *Contro l'idea di costituzione spontanea*, in "Quaderni costituzionali", 2002, n. 1

Clusit (2025), *Rapporto 2025 sulla Cybersecurity in Italia e nel mondo*, 2025

D. Corletto (2003), *Autorità indipendenti e giudice amministrativo*, in P. Cavaleri, G. Dalle Vedove, P. Duret (a cura di), "Autorità indipendenti e Agenzie. Una ricerca giuridica interdisciplinare", Cedam, 2003

V. Crisafulli (1950/2015), *Costituzione e protezione sociale*, in "Rivista degli Infortuni e delle Malattie Professionali", 1950, n. 1, now in V. Crisafulli, "Prima e dopo la Costituzione", Editoriale Scientifica, 2015

B. De Witte (2017), *Exclusive Member States competences: is there such a thing?*, in I. Govaere, S. Garben (eds.), "The Division of Competences between the EU and the Member States: Reflections on the Past, the Present and the Future", Bloomsbury Publishing, 2017

F. Donati (2017), *Democrazia pluralista e potestà normativa delle autorità indipendenti*, in "Osservatorio sulle fonti", 2017, n. 3

P. Eckhardt, A. Kotovskaia (2023), *The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive*, in "International Cybersecurity Law Review", 2023, n. 4

M. Giannelli (2024), *Il contributo dei livelli di governo substatali al raggiungimento degli obiettivi del ddl Cybersicurezza*, in "Rivista italiana di informatica e diritto", 2024, n. 1

W. Gibson (1984), *Neuromancer*, Gollancz, 1984

G. Giraudi, S. Righettini (2002), *Le autorità amministrative indipendenti. Dalla democrazia della rappresentanza alla democrazia dell'efficienza*, Laterza, 2002

T. Giupponi (2023), *Sicurezza e potere*, in "Enciclopedia del diritto. I tematici, vol. V, Potere e costituzione", Giuffrè, 2023

T. Giupponi (2017), *Segreto di Stato (diritto costituzionale)*, in "Enciclopedia del diritto, Annali X", Giuffrè, 2017

T. Giupponi (2010), *Servizi di informazione e segreto di Stato nella legge n. 124/2007,* in "Forum di Quaderni costituzionali", 2010

T. Giupponi (2008), *La sicurezza e le sue "dimensioni" costituzionali*, in "Forum di Quaderni Costituzionali", 2008

H.P. Glenn (2013), *The Cosmopolitan State*, Oxford University Press, 2013

J.L. Goldsmith (1998), *Against Cyberanarchy*, in "University of Chicago Law Review", 1998, n. 4

IBM (2024), *Cost of a Data Breach Report*, 2024

N. Irti (2000), *Economia di mercato e interesse pubblico*, in "Interessi pubblici nella disciplina delle public companies, enti privatizzati e controlli", Atti del XLV Convegno di studi di scienza dell'amministrazione. Varenna, Villa Monastero, 16-18 settembre 1999, Giuffrè, 2000

I. Harun (2017), *Raspodjela nadležnosti prema Ustavu BiH* (Divison of Competences According to the Constitution of Bosnia and Herzegovina). Sveske za javno pravo | Blätter für Öffentliches Recht, 2017

D.R. Johnson, D. Post (1996), *Law and Borders: The Rise of Law in Cyberspace*, in "Stanford Law Review", 1996, n. 5

A. Lauro (2021), *Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione*, in "Rivista Gruppo di Pisa", 2021, n. 3

E. Longo (2024), *Il diritto costituzionale e la cybersicurezza. Analisi di un volto nuovo del potere*, in "Rassegna parlamentare", 2024, n. 2

M. Luciani (2013), *Il segreto di Stato nell'ordinamento nazionale*, in "Gnosis. Rivista italiana di intelligence", 2013, n. 2

M. Luciani (1996), *L'antisovrano e la crisi delle costituzioni*, in "Rivista di diritto costituzionale", 1996, n. 1

M. Manetti (2023), *Poteri e garanzie (Autorità indipendenti)*, in "Enciclopedia del diritto. I tematici, vol. V, Potere e costituzione", Giuffrè, 2023

C.H. McIlwain (1990), *Constitutionalism: Ancient and Modern*, New York, 1947, transl. it. *Costituzionalismo antico e moderno*, il Mulino, 1990

A. Merdzanovic (2016), *'Imposed consociationalism': external intervention and power sharing in Bosnia and Herzegovina*, Peacebuilding, 2016

S. Morgan (2023), *Cybercrime To Cost The World $9.5 Trillion Annually in 2024*, in "Cybercrime magazine", 2023

L. Moroni (2024), *La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, in "federalismi.it", 2024, n. 14

A. Pajno (1996), *L'esercizio di attività in forme contenziose*, in S. Cassese, C. Franchini (eds.), "I garanti delle regole", il Mulino, 1996

M. Pietrangelo (2024), *La dimensione plurale della cybersicurezza: da potere invisibile a processo collaborativo*, in "Rivista italiana di informatica e diritto", 2024, n. 2

S. Poli (2021), *Il rafforzamento della sovranità tecnologica europea e il problema delle basi giuridiche*, in "AISDUE", 2021, n. 5

L. Risicato (2019), *Diritto alla sicurezza e sicurezza dei diritti: un ossimoro invincibile?*, Giappichelli, 2019

A. Riviezzo (2005), *Autorità amministrative indipendenti e ordinamento costituzionale*, in "Quaderni costituzionali", 2005, n. 2

S. Schmitz-Berndt, P.G. Chiara (2022), *One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS 2 directive*, in "International Cybersecurity Law Review", 2022, n. 3

F. Serini (2022), *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in "federalismi.it", 2022, n. 12

M. Siclari (2008), *I mutamenti della forma di governo. Tra modificazioni tacite e progetti di riforma*, Aracne, 2008

A. Simoncini (2022), *La dimensione costituzionale dell'intelligenza artificiale*, in G. Cerrina Feroni, C. Fontana, E.C. Raffiotta (a cura di), "AI Anthology. Profili giuridici, economici e sociali dell'intelligenza artificiale", il Mulino, 2022

H. Tahir, N. Muftić (2023), *Regulation of Audiovisual Media in Bosnia and Herzegovina – an Overview: Is the Cure Worse Than the Disease?*, in G. Gergely, E. Lazar (eds.), "Media Regulation During the COVID-19 Pandemic: A Study from Central and Eastern Europe", Ethics International Press, 2023

U.S. Joint Chiefs of Staff (2011), *Cyberspace, in Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, Washington DC, 2011

P. Zvijerac (2021), *Sve odluke Valentina Inzka*, Radio Slobodna Evropa, 20 July 2021