Private Law Perspectives of Cybersecurity

Federica Casarosa[1, 2, *, †], Giovanni Comandé [2, †]

[1] *Sant'Anna School of Advanced Studies, Piazza dei Martiri 33, 56127 Pisa, Italy*
[2] *European University Institute, Via Boccaccio 121, 50133 Firenze, Italy*

Abstract
Cybersecurity is very rarely related to private law. However, the normative evolution and the growing intertwining of economic and organisational dependencies between entities, economic operators, and public administrations make increasingly evident the mutual influences between the legal area of cyber security with more and more of the substantial structures of private law. The overlaps and the cases of tension between the normative plexuses will be highlighted, as well as the need for linkage and translation of what are legal requirements into technical needs. The conclusions will provide suggestions for regulatory policy and interpretive practices. In the background, the contribution highlights the emergence of an increasingly intricate relationship between the cyber security requirements of value chains and the different levels of standardisation that must be implemented.

Keywords
Cybersecurity, public procurement, supply chain control

1. Introduction

Cybersecurity is very rarely related to private law. However, the normative evolution and the growing intertwining of economic and organisational dependencies between entities, economic operators, and public administrations make increasingly evident the mutual influences between the legal area of cyber security with more and more of the substantial structures of private law.

This contribution highlights these critical interferences, also considering the historical reconstruction of European legislation in its national unfolding until the implementation of the so-called NIS2 directive. The overlaps and the cases of tension between the normative plexuses will be highlighted, as well as the need for linkage and translation of what are legal requirements into technical needs. Then, the conclusions will provide suggestions for regulatory policy and interpretive practices. In the background, the contribution highlights the emergence of an increasingly intricate relationship between the cyber security requirements of value chains and the different levels of standardisation that must be implemented.

ITASEC24: Italian Conference on Cybersecurity, April 08–12, 2024, Salerno, Italy
* Corresponding author.
† These authors contributed equally.
Federica.casarosa@santannapisa.it (F. Casarosa); Giovanni.comande@santannnapisa.it (G. Comandé)
0000-0002-5256-3505 (F. Casarosa); 0000-0003-2012-7415 (G. Comandé)

2. Cybersecurity in the Italian legal framework

Cybersecurity encompasses the strategies and regulations operating at the national and supranational levels to mitigate and respond to any attacks that could undermine the stability and development of businesses and public administrations [4, 10]. While from a practical point of view, we can talk about cybersecurity from the moment computers became connected through the Internet. However, it is only since the late 2000s that legislators' attention and public awareness regarding this issue have emerged. The turning point can easily be attributed to the attack suffered by Estonia's IT infrastructure in 2007, when a series of Distributed Denial of Service (DDoS) attacks succeeded in crippling the infrastructure nationwide [7, 11]. From this moment on, many states have begun to consider the desirability, indeed the necessity, of adopting cybersecurity strategy policies.[2]

While awareness of security risks has increased, cyber-attacks have multiplied, including supply chain attacks, cyber espionage, ransomware, or complete disruption of services [3]. Exposure to cybersecurity incidents and their potential impact is linked to the pervasiveness of the use of ICT in all economic sectors, as governments, businesses, and citizens are more interconnected and interdependent. Moreover, Russia's recent military aggression against Ukraine has shown how cyber operations are increasingly integrated into hybrid warfare strategies, with significant effects on the target [13]. The threat of possible large-scale incidents causing disruption and significant damage to critical infrastructure requires increased preparedness at all levels of the cybersecurity ecosystem.

Italy has recognised cybersecurity risks since the mid-2000s and several legislative interventions have introduced regulations to prevent and mitigate these risks. Observing the evolution of legislative interventions over the past two decades is interesting.

Legislative Decree No. 82 of 2005, the so-called Digital Administration Code, marks the moment of acceleration of the PA's digitalisation process. Article 51 shows an initial intervention on data security, stating that "The security standards defined in the technical rules ... guarantee the accuracy, accessibility, integrity and confidentiality of data" and that "Computer documents of public administrations must be kept and controlled in such a way as to minimise the risks of destruction, loss, or unauthorised access or access not following the purposes of collection". In the same year, Law No. 155/2005 on urgent measures to combat international terrorism was adopted, including Article 7a on cyber security, where the cyber protection services of critical digital infrastructures of national interest were allocated to the Ministry of the Interior, with the enforcement role of the Postal Police in case of cyber-attacks. Critical ICT infrastructures are defined through the criteria and procedures identified in the Decree of January 9, 2008, which includes all systems and

[2] See the interventions adopted in the United Kingdom, The UK Cyber security Strategy: Protecting and Promoting the UK in a Digitalised World (2011); in Austria, the National ICT Security Strategy (2012); in Estonia, the Cybersecurity strategy (2008); in France, the Défense et sécurité des systèmes d'information: Stratégie de la France (2011); and in the Netherlands, the Defence Cyber Strategy (2012). For a comparison of the issues in the respective national legislations and policies [8]. For Italy [1].

services supporting ministries, agencies and entities supervised by them, operating in the areas of international relations, security, justice, defence, finance, communications, transportation, energy, environment, and health.[3] They are joined by the Bank of Italy and independent authorities and companies owned by the state, regions and municipalities in the communications, transport, energy, health and water sectors.

Since the 2010s, interventions related to cybersecurity have intensified, paying greater attention to the specificities that may emerge both from the protection of public administrations and from national defence. In 2012, the so-called Italian Digital Agenda was defined, creating an Agency for Digital Italy (Agenzia per l'Italia Digitale - AgID). The agency, established by Decree-Law No. 83/2012 (converted into Law No. 134/2012), had the task of coordinating "actions in the field of innovation to promote ICT technologies to support public administrations, guaranteeing the realisation of the objectives of the Italian Digital Agenda, in coherence with the European Digital Agenda". The importance of cybersecurity issues ranks among AgID's first strategic actions with the 2013 Digital Agenda Implementation Strategy [12].

The Prime Minister's Decree of January 24, 2013, addressing cyber protection and national cybersecurity, was the first piece of legislation to coordinate cybersecurity-related activities involving public administrations and the intelligence community.[4] Subsequent national strategic documents, the National Strategic Framework for Cyberspace Security and the National Plan for Cyberspace and Cybersecurity defined the internal organisation to enable timely and coordinated responses to cyber threats targeting national assets. What emerges is the need to keep defence strategies continuously updated given the constantly evolving technologies, and on the other hand, the need for a wide-ranging involvement of the actors involved in this process, not only public and private entities but also citizens who can alert on potential cyber threats [2].

In 2016, changes were adopted to comply with Directive 2016/1148 on the security of networks and information systems (NIS Directive), representing the first horizontal legislative intervention undertaken at the European level to protect networks and information systems throughout the Union.

As evident from the preceding analysis, the legislator had to intervene to adapt the pre-existing system to the European standards; however, unlike in other European countries, the impact of the changes was limited since both competencies and organisational structures had already been identified during the previous decade. A significant impetus for improving the existing regulatory framework has been the need to define the requirements for the prevention and resilience of so-called essential services operators. To understand

---

[3] It is important to note that this decree anticipates by almost a year the Directive 2008/114/EC on the identification and designation of European critical infrastructures and assessing the need to improve their protection. The sectors this directive covers are energy and transport, and there was no agreement at the European level to extend them further.

[4] The new organisation provides an apex role to the President of the Council of Ministers and the ministers who comprise the Committee for the Security of the Republic (CISR) with political-strategic tasks. Operational support is then provided by the Inter-Ministerial Committee, chaired by the Director General of the Department of Information for Security (DIS), which carries out both the preparatory activity of the work of the Inter-Ministerial Committee and the coordination between relevant administrations and offices, as well as between them and the public and private entities called upon to implement it.

this framework, it is necessary to briefly analyse the NIS Directive and understand how the Italian legislature has implemented the national cybersecurity strategy.

3. The Network and Information Systems Security Directive

The Network and Information Systems Security Directive 2016/1148 (NIS Directive) has three main pillars:

1. Strengthen strategic cooperation and information exchange at the European level through the creation of a cooperation group and a network of cybersecurity incident response teams (CSIRT network)
2. Require the adoption of national cybersecurity strategic plans at the national level, including the establishment of national competent authorities and CSIRTs for essential services
3. Identify prevention and resilience mechanisms for essential service operators (OESs) and digital service providers (DSPs).

Without going into detail on the specific aspects of each pillar, it is important to stress a set of innovations.

According to Article 7 NIS, each member state must adopt a national framework that includes the national network and information systems security strategy and the designation of authorities responsible for monitoring the implementation of the NIS Directive. The strategy must include several predefined aspects listed in the abovementioned article but free the member states to design their national strategy. This was an important step, as not all member states had already adopted any measure regarding cybersecurity. Articles 8, 9, 11 and 12 of the NIS Directive then identify the authorities and other bodies responsible for monitoring its implementation at national and EU level [6].

The NIS Directive identified two categories of target actors that should be subject to specific obligations: essential service operators (OES) and digital service providers (DSPs). OES are public or private entities operating in sectors relevant to the national economic system (Art. 4 NIS). Within Annex II of the NIS Directive, the sectors identified as essential are listed in detail: energy, transportation, banking, financial market infrastructure, health sector, drinking water supply and distribution, and digital infrastructure. Additional elements are also included in Article 5 NIS.

As a result, not all OES operating in the areas identified in the directive fall within the scope of the directive. It is up to the member states to identify the list of OSEs at the national level. This determination is not made public and remains a state secret to protect the operators themselves from cyber-attacks. The application of uniform criteria in identifying OSEs is essential to consider not only the possible presence of cross-border dependencies but also to ensure a level playing field for operators operating within the internal market and reduce the risk of divergent interpretations.

OES are subject to several reporting obligations and security requirements (Article 14 NIS): OES must take appropriate and proportionate technical and organisational measures to manage risks and prevent and minimise the impact of network and information system security incidents to ensure service continuity. Security requirements are defined by member states and based on a risk-based approach: technical and organisational controls must be appropriate and proportionate based on the risks associated with the type of service performed. However, the Directive does not indicate the methodology for the relevant risk assessments or the technology to use. This is justifiable because identifying a specific approach would risk being quickly obsolete given the rapid developments in the field and because the risk assessment would have to be adapted to different sectors.

According to Art. 14 NIS, OES are required to report, without undue delay, incidents that significantly impact service continuity and service provision, respectively, to the national CSIRT. OES are required to report significant incidents, i.e., incidents that seriously impact the service provided. To identify significant incidents, the directive provides a set of criteria:

- Number of users affected by the interruption of an essential service
- Time interval during which the essential service was not operational
- Geographical extent of the area affected by the incident.

Once the significant incident has been notified, the national competent authority or CSIRT will support the notifying entity in managing the incident. It should be noted that incidents not qualifying as significant are not subject to the notification requirement. The same applies to legal entities not identified as OES. However, in both cases, companies may submit voluntary notifications to the CSIRT of incidents that have a material impact on the continuity of their services.

It should also be noted that these notification requirements are more limited in scope than those for personal data breaches, regulated by the General Data Protection Regulation (GDPR), which must always be notified “unless the personal data breach is unlikely to present a risk to the rights and freedoms of natural persons” (art. 33 GDPR). The different regimes and differences in evaluation criteria in the case of, for example, a data breach that is also relevant as an incident under NIS involving personal data entails different and contradictory organisational and compliance complexities regarding protection requirements and their economic relevance.

This highlights the coordination problem between the notification requirement for cybersecurity incidents and the notification requirement under the GDPR in case of data breaches. Given that, in many cases, a data breach can be at the same time a security incident, the same essential operator acting as a data controller is required to send two different notifications, one to the national CSIRT about the security incident and the other to the Data Protection Authority about the data breach. While in the first case, the obligation must be done "without undue delay," in the second case, the GDPR imposes a specific time constraint of 72 hours after the event is known, with consequent rules for updating information and the need to justify any delay.

4. The Italian implementation

The NIS Directive was transposed into Italian law by Legislative Decree No. 65 of May 18, 2018, which defines the regulatory framework for network and information security measures to be adopted and identifies the entities responsible for implementing the obligations under the European legal framework. However, the Italian state decided to strengthen standards and procedures to ensure a higher level of security of networks, information systems and IT services of public administrations, as well as national public and private entities and operators, through the establishment of the so-called National Cybersecurity Perimeter with the Decree-Law of September 21, 2019 (Perimeter Decree).

In this context, Article 1 (8) Perimeter Decree requires OES and DSP providers to comply with the cybersecurity requirements outlined in Decr. Leg. no. 65/2018, if they are at least equivalent to those established by the Perimeter Implementation Decree. The same article gives the National Cybersecurity Agency the power to define additional measures to meet the security standards established by the Perimeter. The Decree also stipulates that implementing rules to specify further the obligations of those involved will be defined through subsequent legislative interventions, which took the form of four Prime Ministerial Decrees, a Presidential Decree, and a series of acts and communications from various committees.

The Italian government adopted the first D.P.C.M. No. 131 of July 30, 2020, which identifies the public and private entities that fall within the Perimeter and the criteria for creating lists of relevant networks, information systems and IT services of those entities. The second D.P.C.M., No. 81 of April 14, 2021, defines the procedure for reporting incidents and mandatory technical security measures. The third intervention, Presidential Decree No. 54 of February 5, 2021, establishes a procedural framework for the procurement of ICT assets for use on networks, information systems and IT services by entities within the Perimeter; the categories of these assets are further identified by the Prime Ministerial Decree of June 15, 2021.

This discipline of public control over public and private procurement procedures represents another node of interference/interaction between cybersecurity and private law rules. In fact, "prior to the initiation of procurement procedures or, where not provided for, prior to the conclusion of contracts for the supply of ICT goods, systems and services referred to in Article 1, paragraph 6(a)" of DPCM 54/2021, notification must be made to the CVCN or CVs called to perform the tests, referred to in Article 6 and Article 7 but, more importantly, to dictate any "possible conditions and tests of hardware and software to be included in the clauses of the tender or contract, referred to in Article 5, as well as any usage requirements to the entity included in the scope" (Art. 4 paragraph 3). Indeed, some interesting features emerge.

First, it devolves to an administrative authority (technically, the CVCN is an internal articulation of an Agency and not an independent Authority), with the possibility of defining the limits to the private autonomy of the parties. However, such limits are entirely demanded by the administrative authority as no general and abstract definition can be found in the underlying legislation. Parties that do not follow the indications or do not report the procedures/contracts may incur sanctions. In any case, the business transaction,

even possibly entirely private, can be wholly prohibited if the procedure leads to a negative outcome or can be subject to conditions more or less invasive towards contractual and entrepreneurial autonomy (e.g. limitations on use, duration, insertion of contractual clauses).

Given that the inclusion in the National Cybersecurity Perimeter should be a state secret, which should also be maintained in case of contractual transactions that led to a negative or conditional assessment by the CVCN, the economic operator involved in such transaction lies in a complex situation. On the one hand, it should negotiate (and bear the related costs) the content of the clauses, taking into account the limits imposed by the CVCN, and in case of a breakoff of the negotiations (with consequent legal and economic responsibilities), without being able even to explain the reasons. Moreover, should the proposed contract clauses by the CVCN be structured in such a way as not to adequately disguise their founding reasons, the same economic operator would directly or indirectly 'reveal' the inclusion within the Perimeter of the entity involved, with even more significant harm to both state security and to the entity involved. Such framework shows that the procedures and the solutions adopted require skills and practices that have not been developed yet and that lead, on the one hand, to the involvement of private entities in the creation of the general framework of national cyber-physical security and, on the other hand, to the need for an update (perhaps not only) interpretation of several private law rules. As we shall see below, the reference to cyber-physical security is not accidental, given the interrelationship of the two types of security, similar to the repercussions of what has just been emphasised in contractual dynamics.

DPCM No. 131/2020 establishes the procedural criteria by which the relevant public administration shall identify the entities included in the Perimeter. As anticipated, the list of entities in the Perimeter will be included in an administrative act adopted by the Prime Minister, which is not subject to publication. The rationale for secrecy lies in the underlying purpose of protecting national security; however, the secrecy is more formal than real, as most of the entities within the scope of the Perimeter are easily identifiable, as these entities represent the most critical players in the sectors identified by the legislation. Interestingly, Art. 1(5) Perimeter Law and Art. 3(1) Prime Minister's Decree No. 131/2020 provide an element of "flexibility" in terms of adjustments to the national legal framework for cybersecurity: the former establishes a legal basis for updating the implementing decrees, while the latter explicitly provides for the possibility of extending the scope to other sectors when the decree is updated.

Entities within the Perimeter are obliged to prepare a list, updated annually, of the networks, information systems and IT services that constitute the ICT assets under their control. The list must be compiled using a scalable, risk-based approach so that the ICT assets that would cause complete disruption of the essential function or service in the event of an incident are evident. Operators included in the perimeter are then required to describe the architecture and parts of the previously identified ICT assets based on a template provided by the National Information Security Agency. This obligation could prove particularly challenging, especially given the high rate of digitisation of many operators. These lists must be submitted to the Agency within six months of receiving notification of registration in the Perimeter.

The reporting procedure and risk management measures are defined by DPCM No. 81/2021. Information security incidents are classified according to their impact on ICT assets. The provided taxonomy distinguishes two types of incidents based on their severity.[5] This classification is functional to the different time frames required for an effective response: incidents identified in Annex A, Table 2, are to be reported within one hour, while the ones falling in Table 1 should be reported within six hours. These deadlines run from the moment the entity becomes aware of the incident, such as through the monitoring, testing and control activities based on the cybersecurity measures provided for in the same decree.

Regarding IT security measures, Annex B DPCM No. 81/2021 contains a complex and very detailed taxonomy of IT security measures. These measures, which fall under the category of technical controls, are grouped according to their functions: identify, protect, detect, respond and recover. Entities must notify the Information Security Agency without undue delay of adopting such measures; notification is also required for related updates. Interestingly, DPCM No. 81/2021 provides explicitly for aspects related to data security, incorporating the requirements of the General Data Protection Regulation, No. 679/2016. The structure adopted by the legislature to identify cybersecurity measures echoes the Cybersecurity Framework model developed by the National Institute of Standards and Technology (NIST) in 2014 and adopted at the U.S. level to reduce cybersecurity risks. The Italian model is divided, as well as the NIST standard, into five classes. Each function is then divided into categories and subcategories representing the individual controls to be addressed in the risk analysis and assessment. Compared to the U.S. model, the framework of requirements provided at the Italian level is broader because it includes, as mentioned, the subcategories related to implementing regulations related to the protection of personal data. As highlighted in the research carried out as part of the ERACLITO project [5], the legal and technical requirements outlined in the regulations are multiple and detailed, requiring numerous interventions and investments of both technical and organisational nature to the companies that fall under the perimeter to demonstrate compliance.

DL No. 82/2021 established the National Cybersecurity Agency to assume the role of the National Cybersecurity Authority as the single point of contact for the NIS Directive and the National Cybersecurity Certification Authority for the Cybersecurity Act. In this regard, Chapter IV of Presidential Decree No. 54/2021 establishes the supervisory powers and procedures for inspections and audits concerning fulfilling the various obligations imposed by the DPCMs. In addition to periodic monitoring, Chapter IV also provides for ad hoc inspections if deemed necessary in exceptional cases (e.g. as a result of incident notifications, non-compliance with any of the obligations arising from the implementation of the relevant regulations, and notifications from other public authorities). Audit activities are carried out through document analysis and verification.

The Perimeter Decree moreover introduces different administrative penalties for failure to comply with the obligations imposed by the Perimeter Decree and its implementing decrees. For example, failure to comply with the obligation to prepare, update and submit

[5] Table 1 in Annex A contains the less severe incidents (e.g. infection, failure, installation, lateral movement, actions on targets) and Table 2 the more severe ones (e.g. actions on targets and disruption).

lists of networks, information systems and IT services is subject to an administrative penalty ranging from 200,000 to 1.2 million. In contrast, failure to report cybersecurity incidents or implement cybersecurity measures is subject to fines ranging from 250,000 to 1.5 million. Interestingly, harsher penalties are imposed for non-compliance with procurement requirements: an entity that fails to notify the CVCN of its contract for the supply of ICT goods and does not comply with the conditions set by the CVCN can be fined up to 1.8 million. In addition, Article 1(11) Perimeter Decree also provides for the criminal penalty of imprisonment of one to three years for providing false information, data or facts or the failure to report such data in order to hinder or influence the completion of procedures related to incident reporting, cybersecurity management measures, procurement or inspections, and supervisory activities.

5. The evolution of the regulatory framework

As member states worked to implement the NIS Directive, the Commission presented in December 2020 the new legislative instrument aimed at replacing the NIS Directive, overcoming some of the shortcomings of the latter, eventually adopted as Directive 2555/2022 on measures for a high common level of cybersecurity in the Union (NIS 2). NIS 2 still aims to improve security to safeguard the digital internal market by establishing harmonised standards in cybersecurity risk management and incident reporting. This approach is also confirmed by extending the number of areas covered by NIS 2, which will consequently increase the number of entities to which the obligations and requirements will bind. The increased number of entities involved will amplify the interference with contractual autonomy highlighted earlier. However, this is not enough. It is essential to point out that the current structure of NIS 2 is based on evaluation and reporting on the impact of the NIS directive. One of the first challenges that emerged from the structure of NIS 1 was identifying the actors included in the scope. NIS 2 distinguishes between essential entities (EEs) and important entities (IEs) without substantial differences regarding reporting requirements and obligations. The identification criteria have changed: the first criterion is enterprise size, excluding small and micro enterprises from its scope (Art. 2(1) NIS 2). Although the Commission admits that this criterion "is not necessarily an ideal stand-alone criterion for determining the importance and criticality" of an entity, it is a significant proxy for determining whether certain entities play vital roles in society and the economy. While the need to limit the impact of legislation that is challenging for private entities involved is understandable, it remains problematic to prioritise the selection of a quantitative criterion that, despite exceptions, does not present sufficient, objective and flexible criteria capable of weighing the quality of the entity to be involved.

Indeed, the text provides an extensive list of exceptions, which apply regardless of company size. For example, size is irrelevant in the case of services provided by providers of public electronic communications networks or publicly accessible electronic communications services, by providers of trust services, or even by top-level domain name registries and domain name system service providers; in the case of entities that are the sole provider in a member state of service essential to the maintenance of critical social or

economic activities; where the interruption of the service provided by the entity could have a significant impact on public safety, public security or public health; or for public administration entities. The second criterion is activity in one of the sectors identified in Annexes I and II of NIS 2. Interestingly, NIS 2 significantly extends the scope of the NIS Directive, adding new sectors such as telecommunications, social media platforms, and public administration.

It is essential to underline that the size criterion combined with the list of exceptions cannot intercept increasingly topical situations, such as those links included in the production chains whose role does not directly fall within the listed exceptions. Even though such links cannot be qualified as the sole provider of an essential service to the maintenance of critical social or economic activities in a member state, they still represent a bottleneck for the production chain that might bring the link back within the perimeter or even allow the qualification as an essential entity. This observation leads us to anticipate a further regulatory and operational short circuit that can be generated. In fact, in the absence of suitable tools and quality verification criteria to identify bottlenecks in production chains and, perhaps, suitable technical and economic capacity on the part of EEs/IEs, these have net responsibilities in propagating security requirements and obligations along their production and supply chains.

Article 21 (2) requires that security measures include "(d) supply chain security, including security aspects of the relationship between each institution and its direct suppliers or service providers". Paradoxically, EE and IE entities, in addition to being able to identify and implement 'appropriate and proportionate' measures internally to their organisation, are still called upon to address supply chain security. The result is again the imposition of obligations and capabilities to analyse risks and design economic and legal models to govern them on private entities that, despite the regulatory imposition, may not have the capabilities or even awareness. We are unaware of any financial or other modes of assistance to address these actual compliance costs with a high impact on contractual and entrepreneurial autonomy. The practical result, therefore, could lead to both high compliance costs and unsatisfactory levels of compliance effectiveness.

Concerning reporting requirements, NIS 2 provides a two-step approach to incident reporting that overcomes problems arising in implementing NIS. During the first phase, the affected entity must inform, with an initial report, the national authority or CSIRT within 24 hours of becoming aware of an incident. After that, the same entity will provide a full report within 72 hours of becoming aware of the incident. The second stage involves the full recovery of the problem, with a final report to be submitted one month after the initial report.

In terms of enforcement, the directive establishes a minimum list of administrative fines for cases where entities violate the cybersecurity risk management rules or notification requirements under NIS 2. These are then complemented by the powers provided for national authorities, which include warnings, adoption of binding instructions, and implementation of recommendations (Art. 32(4) NIS 2).

6. Open issues and the need for further research

The rapid evolution of the regulatory framework at the European level regarding information security with the adoption of the NIS 2 directive leads to considerations regarding how it should be implemented at the national level.

First, in light of the different levels of detail provided in Art. 21 NIS 2 regarding the measures to be taken by EEs and IEs on information security compared to the laconic indications provided in Art. 14 NIS, it will be necessary for the Italian legislature to assess whether the current requirements in Table B of DPCM No. 81/2021 are sufficient and in line with the provisions of the new legislative framework. Moreover, updating the NIST standard itself is also worth mentioning. In August 2023, the draft of the so-called NIST 2.0 was presented. Again, numerous changes could be relevant, where the Italian legislature wants to maintain an affinity (*rectius* conformity) with the U.S. standard.

A related aspect is the need to harmonise the requirements set by member states for cybersecurity at the European level. While ENISA's supportive and advisory role has made it possible to steer the choices of national governments in the same direction, the presence of even partially different requirements could result in companies offering essential services in more than one member state. In this sense, the role of the Cooperation Group can be an essential framework in which not only to exchange best practices and information regarding the implementation of the directive but also to identify common choices and approaches regarding the security standards to be adopted(Article 14(3)(c) NIS 2).

One of the problematic aspects of NIS 2 is the choice to exclude small and micro enterprises from the scope of application. These entities, considering the size criterion in the directive, are not subject to any obligation to adopt cybersecurity safeguards. Although numerous exceptions relate to the importance and criticality of the services performed by enterprises in the European territory, many remain uncovered. This leads to increased risk, as most micro and small enterprises have fewer economic and organisational resources invested in cybersecurity, but they also become prime targets for cyberattacks. Thus, in this case, it seems essential to use an indirect form of implementing cybersecurity measures through supply chain control. As per Article 21(2)(d), the security measures to be taken by EEs and IEs also include verification of the level of security taken by direct suppliers or service providers. The directive's definition, in this case, does not place any constraints: every type of supplier and provider, regardless of size, industry, and type of products and services offered, is included. This is crucial to ensure that cyber threats and attacks cannot be perpetrated through flaws or vulnerabilities that can be traced back to components used by the EE or IE in their business [9]. From a practical standpoint, therefore, the EE or IE will need to provide for mapping of its suppliers and service providers and apply security measures equivalent to those already taken at the enterprise level. Moreover, such mapping is also critical information for the regulator at the national level: providing for a sharing with the National Cybersecurity Agency of the supply chain would allow the same agency to check for possible overlaps, for example, in the case of suppliers and providers operating with multiple EEs or IEs. Where a cyber threat is focused on a specific component developed by a supplier, it would be possible to anticipate possible controls on other EEs and IEs using the same supplier. In addition, in the case of suppliers or providers not established in the

same European country or outside the European territory, it would be possible to anticipate forms of coordinated control at the European level through the aforementioned Cooperation Group provided for in Article 14 NIS 2.

Suppose these conclusions are valid regarding the policy of law and the implementation of NIS2. In that case, the conclusion that the analysis has allowed us to reach in terms of critical regulatory issues remains, in our opinion, fundamental. This first exercise emphasises the importance of the combined mapping of obligations under cybersecurity regulations and the digitisation framework. This is an essential contribution not only to enable compliance but, more importantly, to enable it in a way that takes advantage of synergies between obligations that can be met with the same resources, avoiding duplication that, in addition to representing a cost, also presents a definite risk of confusion in those called upon to implement them. However, the reasoned mapping of obligations and their recipients and identifying corresponding controls is only a first step in highlighting the new lines of convergence and tension between different and increasingly mutually related regulatory plexuses.

What seems to us to be beginning to emerge is a general regulatory framework for cybersecurity that no longer needs to relate only to allied disciplines related to digitisation and the data society (e.g., the discipline of personal data protection or its governance) but also to general institutes of private law, such as general contract law. Further study will be needed to explore the meanings, limits, and effects of these relationships to identify both interdependencies with general disciplines and institutes (e.g., the pre-contractual liability of the private contracting party who, because of clauses "imposed" by the CVCN does not sign the final) and the new interrelationships that are opening up between specific sectors downstream of the expansions that NIS 2 is making in the regulatory landscape and the system of business-to-business and business-to-national security relationships.

Acknowledgements

The research was carried out in the framework of the PNRR project “SoBigData.it: Strengthening the Italian RI for Social Mining and Big Data Analytics” (CUP B53C22001760006) (F. Casarosa); The research was carried out in the framework of the PNRR project “Partenariato Esteso” SERICS (PE00000014) – Eraclito, Spoke 7, funded by Next Generation EU (G. Comandé).

References

[1] R. Baldoni and L. Montanari (eds), Italian Cyber Security Report, Un Framework Nazionale per la Cyber Security. Research Center of Cyber intelligence and information security - Università di Roma Sapienza, 2015. URL: http://www.cybersecurityframework.it

[2] C. Cencetti, Cybersecurity: Unione europea e Italia. Prospettive a confronto, Editore Nuova Cultura, Roma, 2014.

[3] CLUSIT, Rapporto 2023 sulla sicurezza ICT in Italia, 2023. URL: https://clusit.it/rapporto-clusit/
[4] European Union Agency for Cybersecurity, Definition of Cybersecurity - Gaps and overlaps in standardization, 2015.
[5] ERACLITO project, Deliverable 1.1 Project Requirements, URL: https://www.lider-lab.it/en/eraclito-2/.
[6] A. Lauro, Sicurezza Cibernetica e Organizzazione Dei Poteri: Spunti Di Comparazione, Rivista Gruppo di Pisa, 2021, 529.
[7] M. Lesk, The New Front Line: Estonia under Cyberassault IEEE Security & Privacy, 2007, vol. 5, no. 4, pp. 76-79.
[8] S. Mele, I principi strategici delle politiche di cybersecurity, 2013. URL: https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/principi-strategici-delle-politiche-di-cyber-security.html.
[9] G.D. Mosco, La collaborazione tra imprese per la sicurezza informatica, Labour Law Review, n. 2, 2017, 157
[10] V. Papakonstantinou, Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity? Computer Law & Security Review, 2022, 44, 105653. https://doi.org/10.1016/j.clsr.2022.105653
[11] S.J. Shackelford, Estonia Two-and-A-Half Years Later: A Progress Report on Combating Cyber Attacks Journal of Internet Law, 2010. URL: https://ssrn.com/abstract=1499849
[12] M. Zilianti, Verso un'architettura digitale unica e sicura per la P.A.: il ruolo di AgID e Consip, in LLR, 2017, n. 2, 2017, 81.
[13] L. Zorloni, L'invisibile Cyber guerra della Russia per piegare l'Ucraina, 21 Febbraio 2023. URL: https://www.wired.it/article/ucraina-russia-guerra-attacchi-informatici-malware-ddos-energia/