Reporting potential vulnerabilities: a plea for coordination*

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

[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 undergoing a metamorphosis that increasingly emphasises the blurred boundaries between prevention and response. The analysis shows the importance of identifying risks in terms of vulnerabilities and reacting to them fit into increasingly integrated technical, legal and procedural frameworks. The strategy adopted by the European legislator to enable better management of cybersecurity risks was to include an article dedicated to coordinated disclosure of vulnerabilities. Although both Law No. 90/2024 and Legislative Decree, September 4, 2024, No. 138, implementing the NIS 2 Directive, envisages such preventive procedure, both lack a wider private law dimension. In particular, no guidelines are given as regards the consequences that may occur in terms of liability in case a vulnerability is disclosed. A lack of attention towards these issues could clearly affect the effectiveness of coordinated vulnerability disclosure as a preventive tool.

Keywords
Vulnerability disclosure, liability, supply chain, Italian legislation, NIS 2 Directive.

1. Introduction

In the data society, the relationships between legal rules and expertise are undergoing a dizzying process of cross-fertilization. It is no longer possible to consider in isolation issues related to data analytics, development and use of AI, sharing of data for these purposes, or those relating to legal and ethical compliance. In the process, where infrastructure networks are increasingly needed and become more and more strategic and essential assets for companies, the security of data and their processing from external interference is emerging as a central issue. Meanwhile, cybersecurity is also undergoing a metamorphosis that increasingly emphasizes the blurred boundaries between prevention and response. In this context, identifying risks in terms of vulnerabilities and reacting to them fit into progressively integrated technical, legal and procedural frameworks.

*Joint National Conference on Cybersecurity (ITASEC & SERICS 2025), February 03-8, 2025, Bologna, IT
* Corresponding Author.
† These authors contributed equally.
Federica.casarosa@santannapisa.it (F. Casarosa); giovanni.comande@santannapisa.it (G. Comandé)
0000-0002-5256-3505 (F. Casarosa); 0000-0003-2012-7415 (G. Comandé).

This brief analysis is intended to illustrate the need for operational coordination among adopted regulations that reverberate in the daily routines of agencies and institutions. In particular, it will address how the discovery, disclosure and resolution of vulnerabilities are regulated in the current legal framework, comparing the European and Italian interventions on this topic. First, the attention will be devoted to the rules set forth in the 2022/2055 Directive on the harmonisation of network and information system security (so-called NIS 2 Directive), where, for the first time, a coordinated vulnerability disclosure system is set up. Then, the analysis will focus on the Italian interventions. Let us begin with Law No. 90 of June 28, 2024, on Strengthening National Cybersecurity and Cybercrimes. This intervention preceded the legislation implementing the NIS 2 Directive and aimed at paving the way to such intervention defining the tools and rules aimed at protecting Public Administration entities and updating (and tightening) criminal regulations related to cybercrimes.
Within this framework, the law places a set of obligations on Public Administrations, including those related to vulnerability reports (Article 2 L. 90/2024). However, the approach adopted in this legislation is extremely narrow and does not consider the preliminary steps of vulnerability disclosure, nor the impact that it may have on liability.

Our attention will be then devoted to Legislative Decree, September 4, 2024, No. 138, where additional guidelines were expected by market players. Still, its black letter law only translates the actual content of the NIS 2 Directive. We argue this is a missed opportunity that leaves unsolved several issues regarding the potential liability of market players not only towards the users of their products/services but also across their supply chain.

2. Coordinated vulnerability disclosure: a (problematically) multi-step process

The framework of so-called coordinated vulnerability disclosure (CVD) has been introduced by the NIS 2 Directive [1], [2], [3]..

A first important indication emerges from Article 6 (15) of the NIS 2 Directive, which defines the concept of vulnerability as “a weakness, susceptibility or defect in ICT products or ICT services that can be exploited by a cyber threat.” This definition can be analytically dissected into three main elements: (1) the existence of a flaw or weakness in an ICT product or service; (2) the capacity of attackers to exploit or use the flaw or weakness as a potential entry point; (3) the fact that the exploitation of the vulnerability results in a compromised information security [4]. Thus, any conditions that can be related to defects, misconfigurations and other human errors by operators, or unforeseen conditions in the environment in which a system runs can qualify as a vulnerability [4], [5]. From an IT perspective, it is impossible to rule out entirely the presence of vulnerabilities in a system, as technological evolution allows the discovery of initially unknown flaws or criticalities. To this end, only a frequently repeated Vulnerability Assessment and Penetration Test would provide an appropriately high level of security (prevention). Yet, to date, the actual costs and complexities of carrying out such tests exclude this option as a feasible solution.

Moreover, vulnerability differs from cyber threat, which is defined, pursuant to the Cybersecurity Act (Regulation No. 881 of April 17, 2019), as “any circumstance, event, or action that could damage, disrupt, or otherwise negatively impact the network and

information systems, the users of those systems, and other people" (art. 2(8)). So, vulnerability represents one of the possible circumstances that can pave the way for a cyber threat and, therefore, represents a risk that can result in a security incident with consequences of varying degrees. Metaphorically a vulnerability is a threat in potency. For this reason, vulnerability must be resolved before the threat can materialise, for example, by adopting patches that allow the ICT product or service to be corrected. In any case, it should be kept in mind that vulnerability is a preliminary step before the cyber incident. Thus, compliance obligations with vulnerability handling do not cover all requirements related to cyber incidents, requiring coordination from and for stakeholders.

The strategy adopted by the European legislator to enable better management of cybersecurity risks was to include an article dedicated to coordinated disclosure of vulnerabilities. In fact, Article 12 of the NIS 2 Directive provides for the identification of a national coordinator, the so-called 'cybersecurity incident response team' or Computer Security Incident Response Team (CSIRT, provided for in Article 10 NIS 2 Directive), that acts as an intermediary between the natural or legal person reporting the vulnerability and the potentially vulnerable manufacturer or provider of ICT services or products. Where there are multiple CSIRTs at the national level, only one will be in charge of this coordination activity and should be identified by the national implementing legislation.

The legislation implicitly identifies some phases in the coordinated vulnerability disclosure process: the discovery phase, the communication (intermediated) phase, the resolution or mitigation phase, and the phase of disclosure to third parties or the public of the vulnerability [6].

The discovery phase can be carried out either as part of active control activities, such as a socalled penetration testing or red teaming that allows testing the resilience of a system to possible offensive activities [7], [8]; or as part of research activities by developers or researchers [9]. In the former case, the discovery phase is actually, for some entities, a new discovery (they were either not aware the vulnerability existed and that they had it), while for those already aware of the existence, the only discovery can be that they had the vulnerability in their device or system. The two scenarios have different legal implications at least at the level of liability. Also, in case the vulnerability is disclosed thanks to the activities of individual researchers and developers, criminal and civil liability profiles may emerge Their regulatory framework is left by Article 7 (2) (c) of the NIS 2 Directive to the policy choices of each member state [2], [10]. This is particularly important in the context of what is called 'ethical hacking' by researchers and developers, as, for example, the Italian legislative framework still does not clearly set a boundary between legal and illegal activity when hacking is at stake [7], [11]. Moreover, this has implications not yet well defined in the relationships among different sets of legal rules. For instance, consider a company manufacturing an IoT device that does not discover a vulnerability while fulfilling imposed cybersecurity controls. Still, the vulnerability has already been discovered and communicated to the CSIRT coordinator at the national level by a researcher or an independent developer without being resolved or mitigated. In this case, does the company have any liability for damages caused to the users of the IoT device in the event of a security incident that exploits such vulnerability?

The communication phase involves the CSIRT coordinator, who, on the one hand, collects information about the potential vulnerability, allowing for the possibility of anonymous reporting, and, on the other hand, conveys the communication to the

stakeholders. In this case, the intermediary role played by the CSIRT coordinator is also related to verifying the report and assessing the impact report. Indeed, it is not impossible to assume that a single ICT product or service that is subject to a vulnerability may be used by multiple parties. Thus, the effect of the possible attack could be even multiplied. Multiple possible liability rules could come to the fore. For instance, liability on the ICT producer might arise under the modified product liability directive if the product can be considered defective according to the Updated Product Liability Directive (Directive (EU) 2024/2853 on liability for defective products and repealing Council Directive 85/374/EEC), even before the CSIRT communicates the vulnerability. Of course, duties to fix the vulnerability, alert users and eventually withdraw from the market the ICT product would emerge immediately after the CSIRT coordinator discloses publicly the vulnerability with the mitigation measures.

The resolution stage depends on the nature of vulnerability itself, as it is possible that the same reporting party will point to mitigation measures that could eliminate or reduce the risk of the vulnerability being used by an attacker, e.g., through patching, traffic monitoring, or blocking the service. Again, in this case, does the reporting to the manufacturer, for example, impose disclosure obligations on it with consequent liability and diminution to other users? Possibly not until the CSIRT coordinator discloses publicly the vulnerability with or without mitigation measures.

The disclosure stage to third parties or the public is the last step in this process and the most delicate, as anticipated. Only if the reported vulnerability is resolved, can it be made public; otherwise, disclosure of the vulnerability could also inform potential attackers who were not yet aware of it. Hence, disclosure of the vulnerability could be suspended temporarily to develop an appropriate containment strategy [2]. While this is correct from a technical point of view, from a legal point of view, it opens up the previously anticipated issue of what the liability implications are in the interim between the time of identification and the time of disclosure. For instance, the fact that someone already discovered the vulnerability could trigger the fact that the "defect" was already discoverable leading to defectiveness of the product with all the liability consequences.[2] Given that the Updated Product Liability Directive already includes, within the definition of products,0020 software and related services [12], it is reasonable to foresee that a defect of such products can materialise in a cybersecurity flaw, namely a vulnerability

In addition to this pathway operating at the national level, there is coordination carried out at the European level as well by ENISA, which is required to establish and manage a European database of vulnerabilities, enabling the dissemination of knowledge about discovered vulnerabilities even to entities outside the scope of the directive.

The NIS 2 directive, however, does not associate any sanctions for non-cooperation in coordinated vulnerability disclosure. In fact, participation remains voluntary on the part of those reporting the vulnerability and those whose ICT services or products are potentially vulnerable. However, this does not imply that failure to adopt relevant security patches may not be a sanctionable behaviour. In fact, the manufacturer/provider of ICT services or products which fall under the scope of the NIS 2 Directive is required by Article 21 to take

[2] As regards the definition of defectiveness, see CJEU, C-65/20, VI v Krone-Verlag, ECLI:EU:C:2021:471; Case C-264/21, Keskinäinen Vakuutusyhtiö Fennia v Koninklijke Philips NV, ECLI:EU:C:2022:536; and Joined Cases C-503/13 and C-504/13, Boston Scientific Medizintechnik GmbH v AOK Sachsen-Anhalt — Die Gesundheitskasse (C-503/13), Betriebskrankenkasse RWE (C-504/13), ECLI:EU:C:2015:148.

"appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of the information technology and network systems that such entities use in their activities or in the provision of their services, and to prevent or minimise the impact of incidents for the recipients of their services and for other services." While this is obvious after disclosure, it is not so obvious in the interim phase, effectively creating a liability burden that offloads any slowness on the part of ICT technology producers onto users if actual facts do not trigger general or special liability rules outside the realm of NIS2. In particular, one of the elements to be assessed is precisely "the security of the acquisition, development and maintenance of computer and network systems, including the management and disclosure of vulnerabilities" (see Article 21 (2) lit. e)).

Accordingly, any failure to take vulnerability management measures could lead to the application of sanctions under Article 34 (4) NIS Directive 2. Indeed, it is clear that the party aware of the vulnerability is responsible for any failure to take "appropriate and proportionate technical, operational and organisational measures" to contain the identified vulnerability under NIS2. While this could cause a chilling effect generated by the simultaneous absence of an obligation to cooperate/report and a possible exemption in favour of the timely reporter in informing the CSIRT it does not sort out the issue of the liability under general liability rules (e.g. liability for damages caused to others) or consumer protection (e.g. liability for defective ICT products): an undiscovered or unknown vulnerability does not automatically absolve from liability under different legal frameworks.

Another relevant aspect making complex the overall assessment of the liability issues is that the obligations of manufacturers of ICT products or services pursuant to the NIS 2 Directive also extend towards their supply chain. According to Art. 21 NIS 2, the essential and important entity should adopt measures to ensure "d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers". Let's assume that the vulnerability is discovered in a component provided by one of the suppliers of the regulated entity. In this case, the position of the essential entity is critical: on the one hand, it may be subject to sanctions for the absence of specific controls over its supply chain; on the other, it may be liable for potential damages due to the fact that the ICT product/service put on the market was defective.[3] In the former case, a possible exemption can come for the proof of the execution of tests and activities to verify the absence of vulnerabilities. In this case, the collaboration with the CSIRT coordinator when informed about the vulnerability can be an additional element to be considered in reducing the extent of the sanction applied. In the second case, it is possible that contractual clauses could be inserted in the agreement between the essential entity and the supplier to allocate liability in the case of defects in the supplied components when this is not already covered by the Updated Product Liability Directive.

[3] See in particular, Art. 7(1) Update Product Liability Directive provides that "A product shall be considered defective where it does not provide the safety that a person is entitled to expect or that is required under Union or national law". Note that among the elements to be considered, Art. 7(2)(f) includes also the "relevant product safety requirements, including safety-relevant cybersecurity requirements".

3. Disclosure of vulnerability to the national cybersecurity authority according to L. 90/2024

Article 2 L. 90/2024, for the first time, addresses the issue of vulnerabilities in information systems; however, it only addresses one of the previously identified aspects.

The provision allows the Agency for National Cybersecurity (ACN) to report to public administrations covered by the legislation about specific vulnerabilities to which they are potentially exposed. The reporting is not purely generic, as the legislation provides for the ACN to put forward the remedial actions to be taken. It is important to point out that the article applies not only to the subjects referred to in Article 1 (1) L. 90/2024 (central administrations, the autonomous regions and provinces, large municipalities, large urban public transport companies, and ASLs), but also to the subjects included in the national security perimeter, referred to in Article 1 (2-bis) of D. L. 105/2019; to subjects defined by the previous NIS Directive referred to in Article 3 (1) lit. g) and i), of Legislative Decree 65/2018, as well as to companies providing public communications networks or publicly accessible electronic communications services referred to in Article 40 (3) of Legislative Decree 259/2003.

Following the report, potentially vulnerable parties are required to take the suggested measures within fifteen days. Note that it is possible to delay or avoid taking the measures only in the case of "justified needs of a technical-organizational nature" which must, in any case, be promptly communicated to the ACN. Otherwise, failure or delay in adoption may result in applying the administrative fine of 25,000 to 125,000 euros, provided for in Article 1 (6) of the same law.

Comparing the provision to the previously described coordinated vulnerability disclosure process, it becomes clear that the national legislator focused only on the final stage, dedicated to disclosing vulnerabilities to third parties with a limited scope. Indeed, the text refers to a vulnerability situation that is not generic but specific, on which a mitigation or resolution measure that the ACN itself supports is already available.

It is important to note that the vulnerability disclosure process applies to administrations and other entities subject to the notification requirement of Article 1 (1) of the same law. However, it is possible to imagine that such vulnerabilities are present in ICT services and products that administrations may use but have no direct ability to intervene with regard to software development, for example, in the case of in-house communication software provided by a third party. In this case, any mitigation or resolution measure aimed at modifying a software program error should not be addressed to the administration but to the communications service provider or the software developer. This confirms the distinction reported in literature and practice between 'vendors' (i.e., manufacturers and suppliers of ICT products and services) and 'users' of the same ICT products or services [2], [4]. The proceduralizing of the disclosure process helps to partially address the concerns raised earlier. Clearly, the 15-day period for compliance allocates the risk of subsequent harm to the party called upon to comply. In contrast, in the earlier period, it would likely be the users who would bear any costs of violations unless consumer law for ICT products, for example, would lead to a different solution.

In light of the envisaged coordinated vulnerability disclosure activity, one might think that L. 90/2024 could have anticipated some indications for the subsequent implementation

of Article 12 of NIS Directive 2. Unfortunately, the references to controlled vulnerability disclosure stop at Article 2, and no provision of L. 90/2024 concretely defines the forms by which the ACN can collect reports of potential vulnerabilities from individuals or legal entities, nor the intermediation activity with the parties involved. This lack of additional elements addressing the role of ACN in vulnerability disclosure is also confirmed by the amendments provided by Article 3 L. 90/2024 to Article 7 (1) of Decree-Law No. 82 of June 14, 2021 (converted, with amendments, by Law No. 109 of August 4, 2021) regarding the functions of the ACN. The amendment adds subsection (n-ter) regarding the activity of "collecting, processing and classifying data related to incident notifications received by entities that are required to do so in accordance with the provisions in force. Such data shall be made public as part of the report provided for in Article 14, paragraph 1, as official reference data of cyber attacks brought to entities operating in areas relevant to national interests in cybersecurity". Although it is possible to assume that a security incident is the result of an exploited vulnerability, reducing the list of vulnerabilities that requires disclosure only to those that were exploited would be simplistic and could run counter to the cyber risk prevention objectives envisaged both by European legislation and the objectives of the National Cybersecurity Strategy [13]. This interpretation could contradict the correlations between prevention and response, which should be solved with better coordination between legislative provisions.

By law the ACN is already in charge of awareness-raising activities about the presence (and resolution) of vulnerabilities of products and services through communication on the institutional website of the latest vulnerability mitigation measures.[4] Once again, however, in the absence of a comprehensive procedure and paradoxically, the existence of the service could aggravate the position of smaller users or those with fewer resources to devote, who officially would have a duty to keep informed.

4. Awaiting coordination within legislative interventions

Law No. 90/2024 came at a time of transition: Legislative Decree No. 65 of May 18, 2018, which implemented the European harmonisation legislation on network and information system security (Directive (EU) 2016/1148 of July 6, 2016, on measures for a common high level of network and information system security in the Union) and the numerous related regulatory acts need to be amended and adapted to the new rules under the NIS 2 Directive. L. 90/2024 could have anticipated some aspects that would have later been the object of the implementing legislation and allow the Public Administration to change and adapt its organisational structures in a timeframe appropriate to its internal processes. However, in case of vulnerability disclosure, the intervention has been only partial. While it is appreciated that information sharing is acknowledged as a preventive activity to reduce the risk of cyber-attack (in this case, for confirmed vulnerabilities), it is apparent that no action to enable the Agency to fully perform the role of CSIRT-coordinator as envisioned in Art. 12 NIS 2 Directive was introduced, which is a puzzling result, to say the least.

Shortly after, the Legislative Decree, September 4, 2024, No. 138, implementing the Directive (EU) 2022/2555 on measures for a high common level of cybersecurity in the Union, was adopted. Its art. 16 obsequiously translates the original text of the Directive allocating to

[4] See the updates available at: https://www.csirt.gov.it/contenuti?page=0.

the ACN the role of CSIRT coordinator. The implementing legislation provides the multi-phase process addressing the coordinated vulnerability disclosure. Nevertheless, it still leaves the questions mentioned earlier unanswered. In particular, no guidance is offered as regards the consequences that may occur in terms of liability in case a vulnerability is disclosed: if the vulnerability is qualified as a defect, what are the legal consequences when such a vulnerability is exploited, and a user of the ICT device or service is damaged before the mitigation measures are found? What is the role of an essential or important entity in case a vulnerability is discovered in one of the components of its ICT devices or services? A lack of attention towards these issues could clearly affect the effectiveness of coordinated vulnerability disclosure as a preventive tool.

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) – CybeRights, Spoke 1, funded by Next Generation EU (G. Comandé).

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] "Schmitz e Schiffner - 2021 - Responsible Vulnerability Disclosure under the NIS.pdf." Accessed: Apr. 30, 2024. URL: https://www.jipitec.eu/archive/issues/jipitec-12-5-2021/5495/schmitz_schiffner_pdf.pdf

[2] J. Vostoupal, V. Stupka, J. Harašta, F. Kasl, P. Loutocký, and K. Malinka, "The legal aspects of cybersecurity vulnerability disclosure: To the NIS 2 and beyond," *Computer Law & Security Review*, vol. 53, p. 105988, Jul. 2024, doi: 10.1016/j.clsr.2024.105988.

[3] S. Schmitz-Berndt, "Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive," *Journal of Cybersecurity*, vol. 9, no. 1, p. tyad009, Jan. 2023, doi: 10.1093/cybsec/tyad009.

[4] ENISA, "Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations," Report/Study, Jan. 2016. Accessed: Aug. 01, 2024. URL: https://www.enisa.europa.eu/publications/vulnerability-disclosure

[5] J. E. M. D. S. Brandão, "Toward a Vulnerability Mitigation Model," in *The Oxford Handbook of Cyber Security*, P. Cornish, Ed., Oxford University Press, 2021, pp. 141–160. doi: 10.1093/oxfordhb/9780198800682.013.39.

[6] ENISA, "State of Vulnerabilities 2018/2019 - Analysis of Events in the life of Vulnerabilities," Report/Study, Jan. 2019. Accessed: Aug. 01, 2024. URL: https://www.enisa.europa.eu/publications/technical-reports-on-cybersecurity-situation-the-state-of-cyber-security-vulnerabilities

[7] F. N. Ricotta, “Vulnerability disclosure e penetration testing: questioni da normare,” *Rivista italiana di informatica e diritto*, vol. 6, no. 1, Art. no. 1, May 2024, doi: 10.32091/RIID0144.

[8] F. A. Carneiro Pacheco De Andrade, P. M. Fernandes Freitas, and J. R. De Sousa Covelo De Abreu, Eds., *Legal Developments on Cybersecurity and Related Fields*, vol. 60. in Law, Governance and Technology Series, vol. 60. Cham: Springer International Publishing, 2024. doi: 10.1007/978-3-031-41820-4.

[9] F. M. Teichmann and S. R. Boticiu, “An overview of the benefits, challenges, and legal aspects of penetration testing and red teaming,” Int. *Cybersecur. Law Rev.*, vol. 4, no. 4, pp. 387–397, Dec. 2023, doi: 10.1365/s43439-023-00100-2.

[10] ENISA, “Coordinated Vulnerability Disclosure Policies in the EU,” Report/Study, Apr. 2023. Accessed: Aug. 01, 2024. URL: https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu

[11] G. Fiorinelli and M. V. Zucca, “Is the Road to Hell Paved with Good Intentions? A Criminological and Criminal Law Analysis of Prospective Regulation for Ethical Hacking in Italy and the EU⋆,” in ITASEC 2024 - *Italian Conference on Cyber Security 2024, Proceedings of the 8th Italian Conference on Cyber Security (ITASEC 2024) Salerno, Italy, April 8-12, 2024.*, 2024.

[12] G. Wagner, “Liability Rules for the Digital Age: – Aiming for the Brussels Effect –,” *Journal of European Tort Law*, vol. 13, no. 3, pp. 191–243, Feb. 2023, doi: 10.1515/jetl-2022-0012.

[13] ACN, “Strategia Nazionale di Cybersicurezza 2022–2026,” 2021. Accessed: Aug. 01, 2024. [Online]. URL: https://www.acn.gov.it/portale/documents/20119/87708/ACN+Manuale+Operativo+implementazione+misura-82.pdf/ba48be5f-1e69-6b15-8fb9-2d48e52d0d74?t=1704460313679