The Transnational Dimension of Cybersecurity: The NIS Directive and Its Jurisdictional Challenges

Paula Contreras

Abstract This paper explores the jurisdictional challenges that arise from the transnational dimension of cybersecurity, by analysing and comparing the jurisdictional rules applicable to cross-border actors under the NIS Directive and the NIS 2 Proposal. It also comparatively examines the jurisdictional rules of two other EU regulatory instruments applicable to digital services—the GDPR and the DSA Proposal—that rely on the 'main establishment' connecting factor to allocate jurisdiction to one Member State over the others (one-stop-shop mechanisms). Lastly, it assesses whether the NIS 2 Proposal represents a step forward in addressing the complex jurisdictional challenges created by cybersecurity cases with cross-border elements.

Keywords Cybersecurity · NIS Directive · NIS 2 Proposal · Jurisdiction · One-stop-shop mechanism

1 Introduction

We are witnessing a digital revolution that is transforming every aspect of our lives at a vertiginous pace. This has created enormous opportunities but it has also expanded the threat landscape: a growing number of increasingly sophisticated attackers see in the digital transformation of society an opportunity to steal or cause major disruption by exploiting vulnerabilities [1]. The European Union Agency for Cybersecurity (ENISA), for instance, has recently stated that cyberattacks against critical targets in Europe have exponentially increased during the pandemic, which is not surprising given that an unprecedented number of critical services have gone digital in the rush of a global emergency that made security an afterthought [2].

One important aspect that should not be overlooked is that cyber threats may originate abroad, affect several countries, and target companies that provide cross-border services [3]. This transnational dimension of cybersecurity has profound implications

P. Contreras (✉)
SnT, University of Luxembourg, Esch-Sur-Alzette, Luxembourg
e-mail: paula.contreras@uni.lu

C. Onwubiko et al. (eds.), *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media*, Springer Proceedings in Complexity,
https://doi.org/10.1007/978-981-19-6414-5_18

for the legal concept of jurisdiction, because it makes the notion of territory—the traditional connecting factor to authority and jurisdiction—more problematic [4]. Indeed, as cyberattacks take place across geographical borders, the territorial links become opaque because the physical location of the activities or actors subject to the law may be impossible to pin down to a single country and this creates complex jurisdictional challenges [5].

Against this background, the EU has made cybersecurity one of its central priorities, working actively to develop a regulatory framework that ensures a high common level of the security of network and information systems across the EU. The NIS Directive is a key component of that regulatory framework and constitutes the first piece of comprehensive EU-wide cybersecurity legislation [6]. At present, all Member States (and the UK) have transposed the NIS Directive into their national law, creating a new administrative structure at EU and Member State levels, developing a national cybersecurity strategy, and introducing more detailed provisions in relation to the security of their network and information systems [7]. Additionally, because of the increased digitisation of the internal market in recent years and the surge in cyber-attacks during the pandemic, the EU Commission submitted a proposal to replace the NIS Directive (NIS 2 Proposal), which is currently under trilogue interinstitutional negotiations [8].

2 The Jurisdictional Regime of the NIS Directive

Jurisdiction is a multifaceted term that has different meanings in different contexts, so some conceptual clarifications are imperative. This paper will focus on 'regulatory jurisdiction' which deals with the question of identifying the regulatory body competent to apply its powers in cases with a transnational dimension [5]. In this type of case, regulators from multiple countries could potentially invoke suitable connecting factors to their territories to claim jurisdiction. And, based on the goals that a particular regulatory instrument may have, its jurisdictional rules will define which of those connecting factors will be deemed relevant enough to establish jurisdiction. For instance, some instruments may decide that multiple connecting factors will be equally relevant and thus use separate/concurrent jurisdiction rules; some may establish that one connecting factor will be more relevant than the others and consequently will opt for exclusive/primary jurisdiction rules; and yet, other instruments may combine different types of jurisdiction rules, as it is the case of the NIS Directive.

This section identifies and assesses the jurisdictional rules of the NIS Directive that determine the competent regulator in cases with cross-border elements.

2.1 Regulatory Jurisdiction Over Operators of Essential Services (OES)

Under the NIS Directive, OES are companies providing services in the banking, energy, financial market infrastructure, health, transport, water and digital infrastructure sectors that cumulatively: (a) are essential for the maintenance of critical societal and/or economic activities; (b) depend on network and information systems; and (c) operate at such scale that an incident to their network and information systems would have significant disruptive effects on the provision of such service [9]. The jurisdictional rules applicable to OES must be inferred from Article 5 and Recitals 21 and 24.

According to Article 5, Member States must identify the OES that have an establishment in their territory, and if an entity provides an essential service in two or more Member States, before the decision on the identification is taken, those Member States must engage in consultation with each other. Recital 24 clarifies that the consultation process is intended to help them to assess the critical nature of the operator in terms of cross-border impact, allowing each Member State involved to present its views regarding the risks associated with the services provided.

In addition, Recital 21 provides that for the purposes of identifying OES, establishment implies the effective and real exercise of activity through stable arrangements, irrespective of the legal form of such arrangements. Member States have interpreted this connecting factor in different ways. Just to cite a few examples, Germany considers that there is an establishment if the infrastructure of the company is in its territory [10], while Spain requires that the company has its residence or its registered office within its territory provided that these coincide with the place where the administrative management and the management of its businesses or activities are effectively centralised [11]. For Italy, the defining factor is that the company has an office in its territory [12], while Poland requires that the company has an organisational unit in its territory [13]. These divergent interpretations of 'establishment' can result in some entities being identified as OES in some countries but not in others which, in turn, may result in an uneven level of cyber-resilience between different Member States and lead to distorted competition, as companies of the same nature might be imposed different requirements depending on the Member State where they operate [14, p. 9].

In view of the foregoing, it follows that companies identified as OES will be subject to the jurisdiction of the Member State where they provide essential services. Additionally, if those companies provide essential services in more than one Member State, they will be subject to the jurisdiction of each of those Member States in parallel. Thus, several Member States can concurrently have jurisdiction over the same OES if, for example, it has branch offices—or anything that amounts to an establishment under domestic law—in different Member States [15]. Moreover, as the Directive follows a minimum harmonisation approach regarding OES, Member States are free to impose requirements on OES that are higher than those provided for in the Directive [16]. Consequently, companies identified as OES in more than

one Member State will need to comply with security and reporting requirements that vary greatly across countries.[1]

By way of illustration, Ryanair is headquartered in Ireland and is reportedly the biggest airline in seven EU countries (Ireland, Spain, Italy, Poland, Lithuania, Slovakia and Bulgaria), the second biggest in five more (Portugal, Belgium, Hungary, the Czech Republic and Latvia), and the third biggest in the UK [17, p. 10]. This means that Ryanair could potentially be identified as an OES in 13 different countries, and consequently it would have to interact with the NIS national competent authorities (NCAs, SPOCs, CSIRTs and sector-specific authorities) of each of those jurisdictions. In addition, Ryanair would have to implement the security measures and comply with the reporting obligations specified in the national transposition measures of each of the countries where it provides its services, which may vary in terms of reporting thresholds, timeframes, content and formal requirements, and may even present consistency problems [14, p. 88].

In summary, under the NIS Directive, cross-border OES must deal concurrently with a multiplicity of national competent authorities in each of the different countries where they provide services, and additionally, they need to sort out an uneven landscape regarding applicable security and reporting obligations. Moreover, the national approaches to identify OES are not consistent. This multi-level fragmentation of the internal market can make compliance extremely burdensome and can potentially give rise to divergent implementations of the Directive across the EU.

2.2 Regulatory Jurisdiction Over Digital Service Providers (DSPs)

Under the NIS Directive, DSPs are companies providing the following digital services: online marketplaces, online search engines and cloud computing services [6, Annex III]. According to Recital 48, the NIS directive applies to DSPs because the security, continuity and reliability of those digital services are of the essence for the smooth functioning of many businesses (including OES), and therefore a disruption could prevent the provision of other services that could have an impact on key economic and societal activities in the EU. The jurisdictional rules applicable to DSPs are set out in Article 18 and Recitals 64 and 65.

Unlike OES, DSPs are only subject to the jurisdiction of a single regulator across the EU (one-stop-shop approach) based on where they have their main establishment which in principle corresponds to their head office [6, Art. 18]. Recital 64 clarifies that the physical location of the network and information systems is not the determining

[1] For example, France, Croatia and Romania have made security measures mandatory, while others such as Germany and Italy have published guidelines on security measures. Consequently, there are Member States with more detailed legislation on security measures, while others have just defined some rules. Similarly, based on the country, the reporting timeline varies from 'without undue delay or immediately' to 24 h, while the first written report may need to be submitted from five days after the incident occurred to 4 weeks.

factor of the main establishment. In addition, DSPs that are not established in the EU but that offer services in the EU, need to designate a representative established in one of the EU countries where they offer services, and they will be subject to the jurisdiction of the Member State where the representative is established [6], Art. 24(2)]. Moreover, according to the clarifications provided by the EU Commission, if DSPs not established in the UE fail to designate a representative, all the Member States where they offer services can in principle take actions against them if they infringe their obligations deriving from the Directive [15, p. 35].

The rationale for applying such different jurisdictional rules to OES and DSPs stems from the minimum harmonisation approach adopted for the former and the maximum harmonisation approach adopted for the latter. Indeed, according to the NIS Directive, while OES have a direct link with physical infrastructure, DSPs have a cross-border nature per se that demands a more harmonised approach at the EU level [6, Recital 57]. Furthermore, it can also be hypothesised that OES were left under the jurisdiction of each Member State because of the close link that exists between the cybersecurity of critical services and national security [3, p. 113]. Indeed, it has been pointed out that the minimum harmonisation approach towards OES was adopted in recognition of the fact that the legal systems in some Member States already had in place higher standards than those set in the Directive [14, p. 24].

On the other hand, the maximum harmonisation approach towards DSPs was adopted in view of their cross-border nature and the lower degree of risk they may face [6, Recitals 49 and 57]. Accordingly, DSPs were subject to a light-touch approach that was also based on their rapidly changing nature and their innovative potential. This means, among other things, that requirements applied to DSPs are lighter than those applied to OES and that Member States are not allowed to impose DSPs any further security or notification requirements besides the ones foreseen in the Directive [14, p. 14].

On one side, the one-stop-shop approach applicable to DSPs under the NIS Directive reduces the risk of fragmentation mentioned in the previous subsection because DSPs will be under the exclusive jurisdiction of the regulator of the Member State where their main establishment is located. In turn, this means that DSPs will have to comply only with the security and notification requirements specified in the national transposition measure of the country where they have their main establishment which cannot be stricter than those laid down in the Directive. Undoubtedly, this makes compliance simpler and inconsistencies in the implementation less likely.

On the other side, the one-stop-shop mechanism carries with it a risk of 'regulatory shopping'. Indeed, DSPs could structure their operations to place their main establishment in the Member State where they believe they would receive a more favourable treatment from the regulator. In this sense, for example, many Big Techs have chosen Ireland to set up their European headquarters because they consider that the Irish regulators have a more business-minded approach [18]. Also, DSPs could choose to have their main establishment in the Member States that impose lower

penalties, given that there is great variation in the magnitude of the penalties applicable to infringements of the national transposition measures.[2][14, p. 16] Furthermore, another risk associated with the one-stop-shop mechanism is that it could lead to centralizing oversight around regulators that may not have the adequate technical, financial and human resources to carry out the tasks assigned to them, creating delays and inertia [19].

Finally, since at present most OES rely on cloud computing services for the provision of their services, one important consequence of the current jurisdictional rules of the NIS Directive is that OES and the providers of the cloud services that they rely on, may often be under the jurisdictions of different regulators, and thus, subject to different security and reporting requirements. Clearly, this may create complications for supervision and enforcement [17, p. 13].

3 The Jurisdictional Regime of the NIS 2 Proposal

According to the EU Commission, while the NIS Directive increased the Member States' cybersecurity capabilities, its implementation proved difficult, resulting in fragmentation at different levels across the internal market [20]. Consequently, and in view of the growing threats posed with digitalisation and the surge in cyberattacks during the pandemic, on 16 December 2020, the Commission submitted a proposal to replace the NIS Directive. As of January 2022, the NIS 2 Proposal is under trilogue interinstitutional negotiations.

The NIS 2 Proposal abandons the distinction made between OES and DSPs and, in turn, introduces a distinction between 'essential' and 'important' entities that take into account the level of criticality of the sector or of the type of service, as well as the level of dependency of other sectors or types of services [8, Recital 11]. Both categories are subject to the same risk management requirements and reporting obligations. However, they have different supervisory and penalty regimes.

When it comes to the jurisdictional rules, the NIS 2 Proposal provides that, as a rule, all essential and important entities will fall under the jurisdiction of the Member State where they provide their services. And, if the entity provides services in more than one Member State, it will fall under the separate and concurrent jurisdiction of each of these Member States. In this last case, the competent authorities of the different Member States should cooperate with each other and where appropriate, carry out joint supervisory actions [8, Recital 63].

The jurisdictional regime applicable to essential and important entities under the NIS 2 Proposal is comparable to the one applicable to OES under the NIS Directive with the advantage that it does not rely on the concept of establishment that, as it was mentioned above, can be and has been interpreted in different ways by Member States. Moreover, the NIS 2 Proposal has increased the level of harmonisation of

[2] Note, for example, that, while the maximum applicable fine in Lithuania amounts to approximately EUR 6,000, in the UK, fines can go up to approximately EUR 20,000,000.

security and reporting requirements to facilitate regulatory compliance for entities providing cross-border services [8, p. 2].

According to Article 24 of the NIS 2 Proposal, certain types of entities in the digital infrastructure and digital service providers sectors will be subject only to the jurisdiction of the Member State where they have their main establishment because of their cross-border nature. These entities are DNS service providers, TLD name registries, content delivery network providers, cloud computing service providers, data centre service providers and digital service providers (providers of online marketplaces, online search engines and social networking services platforms).

Article 24.2 clarifies that these entities will be deemed to have their main establishment in the Member State where the decisions related to the cybersecurity risk management measures are taken, which typically will correspond to the place of the companies' central administration in the EU. If such decisions are not taken in any establishment in the EU, the main establishment will be deemed to be in the Member State where the entities have the establishment with the highest number of employees in the EU. Also, if the services are carried out by a group of undertakings, the main establishment of the controlling undertaking will be considered the main establishment of the group of undertakings [8, Recital 64] Additionally, the same rules laid down under the NIS Directive regarding the obligation to designate a representative for entities not established in the EU that offer their services in the EU apply under the NIS 2 Proposal.

The jurisdictional rules described in the two paragraphs above are comparable to the ones applicable to DSPs under the NIS Directive, however, the one-stop-shop mechanism devised under the NIS 2 Proposal presents two significant improvements. First, it applies to a broader range of entities that are inherently cross-border. In this sense, for example, it should be noted that while under the NIS Directive DNS service providers and TLD name registries were considered OES and were subject to a concurrent jurisdictional regime, under the NIS 2 Proposal they will be subject only to the jurisdiction of the 'main establishment' regulator. Second, the NIS 2 Proposal provides more guidance to identify the 'main establishment' reducing the risk of divergent interpretation across Member States and potential clashes among regulators.

3.1 Negotiations Between Co-legislators

On 22 November 2022, the EU Parliament adopted the report of the Committee on Industry, Research and Energy (ITRE) that suggested minor changes to the jurisdictional rules of the NIS 2 Proposal [21]. In particular, the report proposed that for those entities that take the decisions related to cybersecurity outside of the EU, the main establishment should be deemed to be either in the Member State where the entities have the establishment with the highest number of employees in the Union, or the establishment where cybersecurity operations are carried out.

The EU Council, for its part, suggested substantial changes to the NIS 2 Proposal in its negotiating position announced on 3 December 2021. Specifically, regarding the jurisdictional rules, the Council stated that the Member States have expressed concerns with the consequences of having a differentiated jurisdiction for entities in the ICT sector, as proposed by the Commission [22]. Consequently, the Council proposed a compromise text in which the relevant jurisdiction is established based on the type of entities: certain entities will be under the jurisdiction of the Member State where they provide their services, some will be under the jurisdiction of the Member State on the territory of which they are established, and others will be under the jurisdiction of the Member State in which they have their main establishment in the EU [22, Art. 24].

3.2 Stakeholder Consultations

A broad range of stakeholders was invited to share their views on the NIS 2 Proposal. The consulted stakeholders included competent authorities, EU bodies dealing with cybersecurity, operators of essential services, digital service providers, entities providing services outside the scope of the current NIS Directive, trade associations and consumer organisations and citizens [8, p. 5.] Regarding the jurisdictional rules, many stakeholders considered positive that the NIS 2 Proposal broadened the application of the one-stop-shop mechanism, and some stakeholders requested that it was extended also to all digital infrastructure service providers, including to public electronic communication networks (PECN), public available electronic networks (PECS), over-the-top (OTT) communication services and trust services [23]. Conversely, other stakeholders expressed that the one-stop-shop mechanism causes more problems than it solves, and that it makes the supervisory process move slower than if the entities were under the jurisdiction of the Member State in which they provide their services or are established [24, p. 6].

In addition, it was pointed out that the number of employees in a specific establishment should not be the defining factor to identify the main establishment of a company in the EU because it is an arbitrary criterion that does not correspond to any security management rationale. Instead, it was suggested that the establishment that has operational and managerial capabilities to implement cybersecurity measures would be a more suitable alternative to identify the main establishment [23, CCIA, p. 2] Likewise, it was argued that when it comes to groups of companies, the assessment of where risk management measure decisions are taken could prove difficult and arbitrary [24, p. 6].

4 A Comparative Review of Other One-Stop-Shop Mechanisms Based on 'Main Establishment'

This section comparatively explores the jurisdictional rules of two other EU regulatory instruments applicable to digital services that, like the NIS Directive and the NIS 2 Proposal, have introduced one-stop-shop mechanisms using 'main establishment' as the relevant connecting factor to allocate jurisdiction.

4.1 The GDPR One-Stop-Shop Mechanism

Under the GDPR, in principle, each national supervisory authority is competent for processing activities that affect data subjects on its territory [25, Recital 122] However, entities undertaking cross-border data processing are under the primary jurisdiction of the supervisory authority of the Member State where they have their main establishment [25, Art. 56] Article 4 (16) defines the main establishment as the place where the company has its central administration in the EU unless the decisions regarding processing personal data are taken in another establishment which has the power to implement those decisions. Still, in some cases, it will be difficult to identify the main establishment or to determine where decisions about data processing are taken, and accordingly, the former Article 29 Working Party (now the European Data Protection Board) has provided guidance in this regard addressing, for example, the cases of groups of undertakings and joint controllers [26]

It should be noted that some stakeholders have expressly requested that the NIS 2 Proposal refers to the 'main establishment' notion under the GDPR and that it does not create an additional specific NIS–main establishment regime [23, DOT, p. 7] Undoubtedly, a good degree of consistency of concepts between these two instruments is desirable, thus, it seems reasonable to take into consideration the developments of the 'main establishment' concept under data protection law when interpreting the NIS Directive or the NIS 2 Proposal. In this sense, for example, Recital 64 of the NIS 2 Proposal makes use of the guidance provided by the Article 29 Working Party to identify the main establishment in cases involving groups of undertakings.

However, it should not be overlooked that these instruments have distinct protection goals: the GDPR covers privacy and data protection rights concerning personal data of individuals, while the NIS Directive and the NIS 2 Proposal encompass the information security for infrastructures [27, p. 101] These different underlying interests may justify some differences in their jurisdictional regimes. Indeed, under the NIS Directive and the NIS 2 Proposal the jurisdiction allocated to the 'main establishment' regulator is exclusive while under the GDPR it is only primary [28, p. 29] According to the GDPR one-stop-shop mechanism, the 'main establishment' regulator has primary competence to oversee cross-border processing activities but there are situations in which another supervisory authority can be competent to act.

This happens, for example, in cases of mainly national relevance [25, Art. 56(2)] and in urgent cases [25, Art. 66(1)]. Clearly, the rationale behind these two exceptions relates to the need to protect the privacy and data protection rights of individuals in a more effective way.

4.2 The DSA Proposal One-Stop-Shop Mechanism

On 15 December 2020, the EU Commission proposed two legislative initiatives to upgrade the rules governing digital services in the EU: the Digital Services Act (DSA) and the Digital Markets Act (DMA). In particular, the DSA Proposal includes rules for online intermediary services and platforms (online marketplaces, social networks, content-sharing platforms, app stores and online travel and accommodation platforms) that are commensurate to their role and size [29]. The DSA intends to improve the mechanisms for the removal of illegal content and for the effective protection of users' fundamental rights online. It also aims at creating a stronger public oversight of online platforms.

According to the jurisdiction rules set out in Article 40 of the DSA Proposal, a provider will be subject to the jurisdiction of the Member State where its main establishment is located, that is, where the provider has its head office or registered office within which the principal financial functions and operational control are exercised. In addition, providers that are not established in the EU but that offer services in the EU must appoint a legal representative, and they will be subject to the jurisdiction of the Member State where their legal representative resides or is established. Furthermore, all Member States will have jurisdiction in respect of providers that fail to designate a legal representative, provided that the principle of *ne bis in idem* is respected [30, Art. 40].

Additionally, it should be noted that Chap. 4, Sect. 3 of the DSA Proposal provides for an enhanced supervision system applicable to very large online platforms (VLOPs) that in some cases empowers the EU Commission to exercise supervision, investigation, enforcement, and monitoring powers. In those cases, the Digital Coordinator of establishment—that is, the competent national authority of the Member State where the provider of an intermediary service has its main establishment or where its representative resides or is established—is no longer entitled to take any investigatory or enforcement measures in respect of the relevant conduct by the VLOP concerned [30, Art. 51(2)] Therefore, it can be argued that when it comes to VLOPs the jurisdiction allocated to the 'main establishment' regulator under the DSA Proposal is primary (like in the GDPR) and not exclusive (like in the NIS Directive and the NIS 2 Proposal).

Some stakeholders have argued that the allocation of jurisdiction to the EU Commission described above is problematic because it excludes Member States from the most serious cases creating a space for potential democratic deficit in the core of the EU institutional framework [31]. On the other hand, many stakeholders believe that the one-stop-mechanism of the DSA Proposal redresses some of the

issues related to delays and inertia existing in the GDRP's cross-border enforcement system by imposing strict deadlines for the coordinator of establishment to answer a request of investigation and enforcement from other supervisory authorities concerned [19]. In this last regard, it is noteworthy to mention that, unlike the GDPR and the DSA Proposal, the NIS Directive does not contain rules regarding the duty of the 'main establishment' regulator to address requests from concerned authorities of other Member States. For its part, the NIS 2 Proposal introduces a mutual assistance mechanism that, however, does not impose any deadline on the competent regulator [6, Art. 34].

5 Recapitulation and Concluding Remarks

As cyberattacks take place across geographical borders, the territorial links become opaque because the physical location of the activities or actors subject to the law cannot be pinned down to a single country and this creates complex jurisdictional challenges. In that line, this paper identifies the jurisdictional challenges that arise from the application of the NIS Directive and the NIS 2 Proposal to cross-border actors.

The NIS Directive uses concurrent jurisdictional rules for cross-border OES and exclusive jurisdictional rules for DSPs. This means that, while cross-border OES are subject to the jurisdiction of each of the Member States where they provide their services in parallel, DSPs are subject only to the jurisdiction of the Member State where they have their main establishment.

The jurisdictional regime of the NIS Directive presents some limitations that were identified in Sect. 2. In this sense, it was pointed out that under the current rules cross-border OES must deal concurrently with a multiplicity of NIS national competent authorities in each of the different Member States where they are identified as OES, and additionally, they need to sort out an uneven landscape regarding applicable security and reporting obligations. Moreover, the national approaches to identify OES are not consistent. All this creates a multilevel fragmentation of the internal market that can make compliance extremely burdensome and can potentially give rise to divergent implementations of the Directive across the EU.

Regarding DSPs, it was noted that the one-stop-shop mechanism introduced by the NIS Directive carries with it a risk of 'regulatory shopping' given that DSPs could structure their operations to place their main establishment in the Member State where they believe they would receive a more favourable treatment from the regulator or where they would face more lenient penalties. Furthermore, it was pointed out that the one-stop-shop mechanism could lead to centralizing oversight around regulators that may not have the adequate technical, financial and human resources to carry out the tasks assigned to them, creating delays and inertia.

Additionally, it was highlighted that under the current rules, OES and the cloud services that they rely on to provide their services will often be under the jurisdiction

of different regulators and subject to different security and reporting requirements which may create complications for supervision and enforcement.

To tackle some of the challenges mentioned above, the NIS 2 Proposal seeks to revise the differentiated approach taken by the NIS Directive regarding the level of harmonisation in relation to OES and DSPS, and it adjusts the light-touch approach applicable to DSPs. In effect, as pointed out in Sect. 3, under the NIS 2 Proposal, essential and important entities providing cross-border services are subject, as a rule, to the concurrent jurisdiction of the Member States where they provide their services, as it was the case for OES under the NIS Directive. But, unlike the NIS Directive, under the NIS 2 Proposal, both categories are subject to the same risk management requirements and reporting obligations.

Moreover, the NIS 2 Proposal upgrades the one-stop-shop mechanism in two senses. Firstly, it makes it applicable to a broader range of entities in the digital infrastructure and digital service providers sector that are inherently cross-border. And secondly, it provides more guidance to identify the 'main establishment' reducing the risk of divergent interpretation across Member States and potential clashes among regulators.

On the other hand, the jurisdictional regime of the NIS 2 Proposal presents some problematic aspects on its own like the number of employees in terms of determination of main establishment. As outlined in Sect. 2, this is arbitrary because it does not correspond to any security management rationale. Likewise, when it comes to groups of companies, the assessment of where risk management measure decisions are taken could prove difficult and arbitrary because there may be cases where multiple establishments within the group make autonomous decisions in that regard.

In the context of the ongoing trilogue negotiations, both the EU Parliament and the EU Council have suggested changes to the jurisdictional rules of the NIS 2 Proposal. This evidences a broad consensus on the necessity and importance of designing a jurisdictional regime that addresses the shortcomings of the NIS Directive and that is in line with the EU Cybersecurity Strategy for the Digital Decade [32].

While the one-stop-shop-mechanisms designed under the NIS Directive, the NIS 2 Proposal, the GDPR and the DSA Proposal rely on the 'main establishment' connecting factor to allocate jurisdiction to one Member State over the others, significant differences among them have been identified in Sect. 4. These differences relate to the different protective goals of those instruments.

Furthermore, the one-stop-shop mechanism under the DSA Proposal seeks to redress some of the shortcomings arising from the GDPR cross-border enforcement by imposing strict deadlines for the 'main establishment' regulator to respond to the requests of concerned authorities from other Member States. Nevertheless, no equivalent provisions are found in the NIS Directive or the NIS 2 Proposal which appears as a missed opportunity by the Commission to take advantage of the lessons learnt from the much-discussed GDPR enforcement challenges.

In summary, it can be concluded that the jurisdictional regime of the NIS 2 Proposal represents a step forward in addressing some of—but not all—the jurisdictional challenges present in the NIS Directive. Moreover, it is possible to argue that

the harmonisation of the security and reporting requirements applicable to essential and important entities is key for redressing (at least partially) those challenges.

Acknowledgments The research for this article was funded by the Luxembourg National Research Fund (FNR) C18/IS/12639666/EnCaViBS/Cole, https://www.fnr.lu/projects/the-eu-nis-directive-enhancing-cybersecurity-across-vital-business-sectors-encavibs/.

References

1. BSA: EU cybersecurity dashboard: a path to a secure European cyberspace (2015). https://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf. Accessed 20 Mar 2022
2. Paton Walsh, N.: Serious cyberattacks in Europe doubled in the past year, new figures reveal, as criminals exploited the pandemic (2021). https://edition.cnn.com/2021/06/10/tech/europe-cyberattacks-ransomware-cmd-intl/index.html. Accessed 20 Mar 2022
3. Internet & Jurisdiction Policy Network: Internet & jurisdiction global status report 2019 (2019). https://www.internetjurisdiction.net/uploads/pdfs/GSR2019/Internet-Jurisdiction-Global-Status-Report-2019_web.pdf. Accessed 20 Mar 2022
4. Svantesson, D.J.B.: Solving the Internet Jurisdiction Puzzle. Oxford University Press, Oxford (2017)
5. Hornle, J.: Internet Jurisdiction Law and Practice. Oxford University Press USA – OSO, Oxford (2021)
6. Directive 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) (2016) Official Journal L 194/1
7. Papakonstantinou, V.: Cybersecurity as praxis and as a state: the EU law path towards acknowledgement of a new right to cybersecurity? Comput. Law Secur. Rep. 2022–04 **44**
8. EU Commission: Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (NIS 2 Proposal), COM/2020/823 final (2020)
9. Weber, R.H., Studer, E.: Cybersecurity in the internet of things: legal aspects. Comput. Law Secur. Rep. 2016–05 **32**
10. § 2 X BSI Act and § 1 I no. 1 Regulation for Determining Critical Infrastructures pursuant to the BSI Act (BSI-KritisV) of 22 April 2016
11. Royal-Decree-Law 12/2018 of 7 September on Security of Network and Information Systems, Art. 2
12. Legislative Decree of 18 May 2018, no. 65, Implementation of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 promulgating measures for a high common level of security of network and information systems across the Union, Art. 4
13. National Cybersecurity Act of 5 July 2018, Art. 5
14. EU Commission (2021) Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)—No. 2020–665, Final Study Report
15. Communication from the EU Commission to the Parliament and the Council (2017) Making the most of NIS—towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, COM(2017) 476 final, Annex 1
16. EU Commission: Report to the Parliament and the Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems, COM/2019/546 final

17. Michels, J.D., Walden, I.: How safe is safe enough? Improving cybersecurity in Europe's critical infrastructure under the NIS Directive. Queen Mary School of Law Legal Studies Research Paper No. 291/2018 (2018). https://ssrn.com/abstract=3297470. Accessed 20 Mar 2022
18. Simmons & Simmons: Ireland's balance between Big Tech and data privacy (2021). https://www.simmons-simmons.com/en/publications/ckucpnrme21dy0a42mwuhhhae/ireland-s-balance-between-big-tech-and-data-privacy. Accessed 20 Mar 2022
19. Vergnolle, S.: Enforcement of the DSA and the DMA. What did we learn from the GDPR? (2021). https://verfassungsblog.de/power-dsa-dma-10/. Accessed 20 Mar 2022
20. EU Parliament: The NIS2 Directive. A high common level of cybersecurity in the EU (2021). https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf. Accessed 20 Mar 2022
21. EU Parliament: Report on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM(2020)0823 – C9–0422/2020 – 2020/0359(COD)), A9–0313/2021 (2021). https://www.europarl.europa.eu/doceo/document/A-9-2021-0313_EN.pdf. Accessed 20 Mar 2022
22. EU Council: Draft Directive on measures for a high common level of cybersecurity across the Union – Council general approach (2021). https://data.consilium.europa.eu/doc/document/ST-14337-2021-INIT/en/pdf. Accessed 20 Mar 2022
23. DOT Europe: Position paper on NIS 2 (2021). https://doteurope.eu/wp-content/uploads/2021/04/DOTEurope_NIS2_PP_Final.pdf. Accessed 20 Mar 2022. Computer & Communications Industry Association (CCIA): NIS 2 Directive. CCIA Europe Comments (2021). https://www.ccianet.org/wp-content/uploads/2021/04/2021.04.23-CCIA-position-paper-on-the-proposed-NIS2-Directive.pdf. Accessed 20 Mar 2022.
24. PTS: Memorandum regarding PTS' positions on NIS 2 proposal (2021). https://pts.se/globalassets/startpage/dokument/bransch/internet/nis/memorandum-regarding-pts-positions-on-nis-2.pdf. Accessed 20 Mar 2022
25. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (2016) Official Journal L 119/1
26. Article 29 Data Protection Working Party: Guidelines for identifying a controller or processor's lead supervisory authority. WP244 rev.01 (2017)
27. Schmitz-Berndt, S., Schiffner, S.: Don't tell them now (or at all)—responsible disclosure of security incidents under NIS Directive and GDPR. Int. Rev. Law Comput. Technol. 2021–2 **35** (2021)
28. Walden, I., Michels, J.D.: Getting critical: making sense of the EU cybersecurity framework for cloud providers. In: Andrader, F., Abreu, J., Freitas, P. (eds.) Legal Developments in Cyber-Security and Related Fields, Forthcoming. Springer. Preprint (2022). https://arxiv.org/pdf/2203.04887.pdf. Accessed 20 Mar 2022
29. EU Commission: The Digital Services Act: ensuring a safe and accountable online environment (2022). https://ec.europa.eu/info/digital-services-act-ensuring-safe-and-accountable-online-environment_en. Accessed 20 Mar 2022
30. EU Commission: Proposal for a Regulation of the EU Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final (2020)
31. Pirkova, E.: The EU Digital Services Act won't work without strong enforcement (2021). https://www.accessnow.org/eu-dsa-enforcement/. Accessed 20 Mar 2022
32. EU Commission: Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final (2020)