Computer Law & Security Review 53 (2024) 105961

Contents lists available at ScienceDirect

Computer Law & Security Review: The International Journal of Technology Law and Practice

journal homepage: www.elsevier.com/locate/clsr

Towards a right to cybersecurity in EU law? The challenges ahead

Pier Giorgio Chiara

Department of Legal Studies, CIRSFID-ALMA AI, University of Bologna, via Galliera 3, 40121 Bologna, Italy

ARTICLE INFO

Keywords:
EU law
EU cybersecurity law
Cyber resilience act
Right to cybersecurity

ABSTRACT

This article aims to engage with the scholarly debate on the introduction of a new fundamental right to cybersecurity in EU law. In particular, the legal analysis focuses on three legal challenges brought about by a theoretical framework for development of a new right to cybersecurity. They regard: i) the need for a new right to cybersecurity against the background of the existing fundamental right to security (Art. 6 EU Charter of Fundamental Rights, CFR); ii) the actual content of this new right; and, iii) how such a new right could be implemented. The article concludes by advocating for the need of acknowledging a new right to cybersecurity in EU law.

1. Introduction

The increasing digitisation informing our time progressively permeates the infrastructure of every sector of society, from transport, energy and telecommunications to health, finance, space and so forth. Public and private actors operating in these sectors, that are pivotal to the Internal market, rely on increasingly interconnected networks, information systems and devices.

In view of the progressive interaction between the digital and physical dimensions, the so-called 'Internet of Things' (IoT) i.e., devices connected to the Internet that continuously interact with physical reality through sensor and actuator systems[1] (according to the international telco industry association GSMA, there will be 25 billion of them on the planet by 2025) ,[2] makes the boundaries between these once clearly distinct realities increasingly blurred.

This paradigmatic transformation brings with it undeniable benefits and opportunities; on the other hand, the widening and interpenetration of the digital dimension into the physical dimension also entails an increase in vulnerabilities to cyber-attacks and -incidents. The threat landscape, progressively increasing both quantitatively and qualitatively, is constantly evolving.[3]

In this context, the concept of 'cybersecurity' – alongside cyber related concepts such as cyber resilience[4] – is continuously being redefined and shaped,[5] also as a governance issue, at national, supranational (e.g., EU) and international (e.g., UN) levels.[6] In EU law, cybersecurity is defined as "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats".[7]

Against an epistemological background where cybersecurity plays an increasingly crucial role for the safety and security of individuals, at present, EU law does not grant individuals with an autonomous 'right to cybersecurity', nor cybersecurity does figure as a policy field in the EU Treaties. For there is not an explicit legal basis for EU policy in this regulatory area, pursuant to the principle of conferral enshrined in

E-mail address: piergiorgio.chiara2@unibo.it.

[1] Recital 14 of the EU Commission's Data Act proposal can provide a functional reference point for a definition of the IoT, amidst the plethora of attempts to framing this enabling technology i.e., "physical products that obtain, generate or collect, by means of their components, data concerning their performance, use or environment and that are able to communicate that data via a publicly available electronic communications service".

[2] GSMA, "The Internet of Things by 2025", see https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf.

[3] ENISA, "ENISA Threat Landscape 2022", https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

[4] Lee A Bygrave, 'Cyber Resilience versus Cybersecurity as Legal Aspiration' in T Jančárková, G Visky and I Winther (eds), *14th International Conference on Cyber Conflict, CYCON* (NATO CCDCOE 2022); Myriam Dunn Cavelty, Christine Eriksen and Benjamin Scharte, 'Making Cyber Security More Resilient: Adding Social Considerations to Technological Fixes' (2023) 26 Journal of Risk Research 1.

[5] Michael Veale and Ian Brown, 'Cybersecurity' (2020) 9 Internet Policy Review 1. See also Vagelis Papakonstantinou, 'Cybersecurity as Praxis and as a State: The EU Law Path towards Acknowledgement of a New Right to Cybersecurity?' (2022) 44 Computer Law and Security Review vis-à-vis the distinction cybersecurity as praxis and cybersecurity as a state.

[6] André Barrinha and G Christou, 'Speaking Sovereignty: The EU in the Cyber Domain' (2022) 31 European Security 356.

[7] Regulation (EU) 2019/881, Art. 2(1).

https://doi.org/10.1016/j.clsr.2024.105961

Article 5 TEU, limiting Union's competences quantitatively and qualitatively.[8]

Eventually, in 2013 the Commission and the High Representative of the Union for Foreign Affairs and Security Policy issued the first Union's strategy for cybersecurity,[9] formally establishing – through this comprehensive policy document – cybersecurity as a new EU policy area.[10]

Since the adoption of the first EU Strategy on cybersecurity, the legal basis for EU policy in this area has been predominantly the functioning of the internal market in accordance with Art. 114 TFUE on the harmonisation of national rules regarding the establishment and functioning of the internal market.[11] The 2013 Strategy highlights that a multi-stakeholder model of governance, based on public-private cooperation, with a view to tackling cyberthreats, "will strongly support the good functioning of the internal market and boost the internal security of the EU".[12] The internal market rationale underlies Directive (EU) 2016/1148 on network and information systems security (NIS Directive) as well, which is widely acknowledged as the first piece of EU legislation on cybersecurity.[13] For it considers that the security of network and information systems is essential for the smooth functioning of the internal market, provided that "network and information systems, and primarily the internet, play an essential role in facilitating the cross-border movement of goods, services and people".[14]

This article intends to contribute to the on-going scholarly debate on acknowledgment of a new right to cybersecurity.[15] The remainder of this article is organised as follows. Section 2 analytically explores the rationale behind the introduction of a new right to cybersecurity in EU law. In connection to that, it casts light on the normative benefits underlying a revision of the EU Treaties with a view to mandating the EU to regulate this fundamental right. Section 3, then, aims to break down the actual content of this new right and discusses whether the European Declaration on Digital Rights and Principles for the Digital Decade, in particular, having regard to the Chapter on 'a protected, safe and secure digital environment' can be used as a reference point for shaping the normative content of such right. Finally, Section 4 focuses on EU secondary law seeking to assess whether and to what extent the horizontal cybersecurity rules for products with digital elements laid down in the proposed Cyber Resilience Act, on the one hand, and the NIS2 Directive, on the other hand, can implement such new right – as outlined in Section 3. In summing up the main findings of this contribution, Section 5 concludes by making a plea for acknowledging a new right to cybersecurity in EU law.

2. Paving the way for a new right to cybersecurity

2.1. Disentangling cybersecurity from security

The main question this section shall be occupied answering with is why a new fundamental right to cybersecurity in EU law is even needed. Preliminary to that, however, is whether the existing fundamental right to security would not be enough to encompass the legal challenges that a right to cybersecurity aims to solve. This would then lead to a more general reflection on the concepts of security and cybersecurity.

One important legal issue raised by a theoretical framework for the introduction of a new right to cybersecurity in EU law is whether an amendment to the existing general right to security,[16] or an extensive interpretation thereby extending its traditional application to the digital sphere, would not be enough to address the identified problem.

Without dwelling on the contextual difficulties of defining cybersecurity and security,[17] we build on the assumption that cybersecurity aims to protect from digital threats, whereas security is preoccupied with the analogical sphere. Papakonstantinou observes in this regard that "while a time may well be imagined that the real and the digital converge, until such time cybersecurity and security, although sharing the same linguistic root and interpretational difficulties, should be treated as two different concepts and rights, each to be assessed by its own merit".[18]

Although the strain of argument above is hardly disputable, one counterargument can nevertheless be raised. The 'Internet of Things' (IoT), and cyber-physical systems in general, brings about a paradigm shift, for it intertwines cybersecurity and security (and safety) more than ever before. The IoT blurs the boundaries between the *digital* and the *physical.* IoT ubiquitous computing renders the physical – virtual dichotomy rather anachronistic, as, in the words of Floridi, "we no longer live online or offline but onlife, that is, we increasingly live in that special space, or infosphere, that is seamlessly analogue and digital, offline and online".[19] This increasingly leads to addressing traditional notions of cybersecurity, security and safety in a more interchangeably or unified way.[20] The hyper-connectedness of *every* social sphere, of the market, brought by the IoT shows the dependence of "human safety on encryption, authentication, data integrity, availability, and other dimensions of cybersecurity".[21] Thus, risk factors and threats in today's *digital-physical* environment go beyond the technological infrastructure

[8] Robert Schütze, 'EU Competences: Existence and Exercise' in Damian Chalmers and Anthony Arnull (eds), *The Oxford Handbook of European Union Law* (Oxford Academic 2015).

[9] European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", JOIN/2013/01 final.

[10] Gloria González Fuster and Lina Jasmontaite, 'Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights' in Markus Christen, Bert Gordijn and Michele Loi (eds), *The Ethics of Cybersecurity*, vol 21 (Springer, Cham 2020) 98.

[11] Jed Odermatt, 'The European Union as a Cybersecurity Actor' in Steven Blockmans and Panos Koutrakos (eds), *Research Handbook on EU Common Foreign and Security Policy* (Edward Elgar Publishing 2018) 359. See also Ana Paula Brandão and Isabel Camisão, 'Playing the Market Card: The Commission's Strategy to Shape EU Cybersecurity Policy' (2022) 60 Journal of Common Market Studies 1335; Helena Carrapico and André Barrinha, 'The EU as a Coherent (Cyber)Security Actor?' (2017) 55 Journal of Common Market Studies 1254, 1259.

[12] European Commission and the High Representative of the Union for Foreign Affairs and Security Policy (n 9) p. 5. See also Brandão and Camisão (n 11) 1345.

[13] Regulation (EU) 2019/881, recital 15; European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" JOIN/2017/0450 final, 7.

[14] Directive (EU) 2016/1148, recital 3.

[15] Vagelis Papakonstantinou, 'Cybersecurity as Praxis and as a State: The EU Law Path towards Acknowledgement of a New Right to Cybersecurity?' (2022) 44 Computer Law and Security Review; for discussion Luca Tosoni, 'The Fundamental Right to (Cyber) Security: A Critical Appraisal of Article 6 CFREU' (Ph.D. diss., University of Oslo, 2022), forthcoming.

[16] EU Charter of Fundamental Rights, Art. 6: 'everyone has the right to liberty and security of person'.

[17] George Christou, 'Conceptualising Security as Resilience in Cyberspace', *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy* (Palgrave Macmillan 2016); Bygrave (n 4); Myriam Dunn Cavelty, Mareile Kaufmann and Kristian Søby Kristensen, 'Resilience and (in)Security: Practices, Subjects, Temporalities' (2015) 46 Security Dialogue 3; Dunn Cavelty, Eriksen and Scharte (n 4).

[18] Papakonstantinou (n 5) 7–8.

[19] Luciano Floridi, 'Soft Ethics and the Governance of the Digital' (2018) 31 Philosophy & Technology 1, 1.

[20] Anton Vedder, 'Safety, Security and Ethics' in Anton Vedder and others (eds), *Security and Law* (Cambridge, Antwerp, Chicago: Intersentia 2020) 21; Marilyn Wolf and Dimitrios Serpanos, *Safe and Secure Cyber-Physical Systems and Internet-of-Things Systems* (Springer 2020) 35–36.

[21] Laura Denardis, *The Internet in Everything - Freedom and Security in a World with No Off Switch*, vol 148 (1st edn, Yale University Press 2020) 184.

of information systems, networks and the underlying information. Cyberattacks could also infringe individuals' fundamental rights, impair physical safety[22] and have critical consequences for services, institutions and communities.

From an epistemological perspective, this strand of arguments pointing at the increasingly convergence of the concepts of security, cybersecurity and safety might hold in favour of an amendment of the general right to security to also cover cybersecurity challenges. This would align with the 'normative equivalency paradigm',[23] which relies on the assumption that traditional human rights can sufficiently embrace the challenges brought about by the digital domain.[24]

The question, however, is setting the right level of abstraction (LoA).[25] Thus, it is not entirely unreasonable to view cybersecurity as a set of activities concerned with the protection of the physical dimension as well. If the designated LoA is cybersecurity's scope of protection, then, one could argue that cybersecurity is a subset of security, for both of them ultimately concern the protection of individuals in the physical and in the digital spheres. Therefore, "there would be no need for a new right to cybersecurity because the general right to security is enough".[26]

However, if we were to shift the LoA to the normative (i.e., legal, ethical and societal) and technical challenges (e.g., in terms of threats) facing cybersecurity and security, we would end up with a different outcome, for the legal means traditionally adopted in the physical dimension to safeguard the interests' protected by 'security' do not translate in the digital sphere. This line of reasoning is confirmed if we turn to EU secondary law in the field of cybersecurity.

Thus, recent legislative developments clearly show a separation of the domains of physical security and cybersecurity. Directive (EU) 2022/2555 (NIS2) and Directive (EU) 2022/2557 (CER) have been presented together by the Commission in December 2020 within the framework of the EU Cybersecurity Strategy for the Digital Decade. The latter directive concerns the resilience of critical entities vis-à-vis physical security, without touching upon cybersecurity which is already addressed in Directive (EU) 2022/2555.[27] At the same time, the CER Directive acknowledges the importance of cybersecurity for the resilience of critical entities and the complementary relationship between physical security and cybersecurity.[28] Member States are therefore called upon to implement the two directives in a coordinated manner, thereby ensuring a coherent approach.

Moreover, an extensive interpretation of Art. 6 CFR on security to include cybersecurity, from a strictly legal standpoint, seems not a viable path. The rights in Article 6 EU CFR "are the rights guaranteed by Article 5 of the ECHR […] and they have the same scope".[29] And art. 5 ECHR – as consistently interpreted by the ECtHR – cannot at present stage be interpreted to include cybersecurity.[30] Thus, Art. 5 ECHR is geared towards protecting the physical liberty of the person by ensuring that no one is deprived of that liberty arbitrarily.[31] In conclusion, Art. 6 CFR cannot be enforced to effectively protect individuals from cyber threats.

2.2. What for a new right to cybersecurity?

Before examining the possible content of this new right (Section 3) and whether remedies exist in EU cybersecurity law for individuals if the addressees of cybersecurity legislation infringe the legal duties they shall comply with (Section 4), account has to be given to the normative question why a new fundamental right to cybersecurity is needed.

Against the background of the broad definition given in Art. 2(1) of the Cybersecurity Act, cybersecurity serves to protect also "persons affected by cyberthreats", and not only network and information systems. In light of the outcomes of Section 2.1, individuals' legitimate expectation to enjoy a 'secure digital life' is not *expressively* and *comprehensively* safeguarded by any EU fundamental right.

It is not contentious that EU data protection law does not legally qualify breaches of (digital) security *per se*. The GDPR in fact covers security breaches only to the extent they lead to "an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".[32]

The breach of technical and organisational security measures[33] can lead to serious detrimental effects, in terms of harms, to individuals even if personal data are not involved in the incident or attack. Thus, cyberattacks or incidents can lead to financial losses (e.g., individuals' devices rendered unusable due to a ransomware attack only impacting the functionality of the system) or psychological distress for individuals. However, if personal data are not impacted, these harms do not amount to violations of the right to personal data protection enshrined in Art. 8 of the Charter. A new fundamental right to cybersecurity would need to provide for such emergent need of protection.

This point admittedly opens up paths for future EU cybersecurity rights-based legal instruments. However, it is questionable whether future EU action in the cybersecurity field can be implemented under Art. 114 TFEU alone, given that EU laws can be enacted under Art. 114 TFEU if there are obstacles to market integration.[34] Moreover, the

[22] 'Internet of Medical Things' (IoMT) is a prominent example of how cybersecurity is progressively taking into account safety considerations as cybersecurity technologies must ensure the integrity of life against cyber (or digital) attacks.

[23] Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2011) A/HRC/17/27; see Dafna Dror-Shpoliansky and Yuval Shany, 'It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights-A Proposed Typology' (2021) 32 European Journal of International Law 1249, 1252.

[24] Cristina Cocito and Paul De Hert, 'The Transformative Nature of the EU Declaration on Digital Rights and Principles: Replacing the Old Paradigm (Normative Equivalency of Rights)' (2023) 50 Computer Law & Security Review 3.

[25] Luciano Floridi, 'The Method of Levels of Abstraction' (2008) 18 Minds and Machines 303.

[26] Papakonstantinou (n 5) 7.

[27] Art. 1(2), recital 9, Directive (EU) 2022/2557.

[28] Recital 9; 24, Directive (EU) 2022/2557.

[29] EXPLANATIONS RELATING TO THE CHARTER OF FUNDAMENTAL RIGHTS (2007/C 303/02), Official Journal of the European Union 3.

[30] European Court of Human Rights, 'Guide on Article 5 of the European Convention on Human Rights: Right to Liberty and Security' (2022) <https://www.echr.coe.int/Documents/Guide_Art_5_ENG.pdf> accessed 3 July 2023.

[31] ECtHR, *De Tommaso v. Italy* [GC], 2017, § 80; ECtHR, *Creangă v. Romania* [GC], 2012, § 92; ECtHR *Engel and Others v. the Netherlands*, 1976, § 58.

[32] Art. 4(12), Regulation (EU) 2016/679. Similarly, albeit with different outcomes, Alunge proposes a modification of the definition of personal data breach in the GDPR to address the limitation of "risky breaches of security" which may not be followed by an ascertained personal data breach, see: Rogers Alunge, 'Breach of Security vs Personal Data Breach: Effect on EU Data Subject Notification Requirements' (2021) 11 International Data Privacy Law 163.

[33] Art. 32, Regulation (EU) 2016/679. See Opinion of AG Pitruzzella delivered on 27 April 2023 (ECLI:EU:C:2023:353) on the CJEU Case C-340/21, concluding that the mere existence of a 'personal data breach' is not in itself sufficient to conclude that the technical and organisational measures implemented by the controller were not 'appropriate' [para. 84].

[34] CJEU Case C-376/98, *Germany v Parliament and Council (Tobacco Advertising I),* ECLI: EU:C:2000:544; CJEU Case C-547/14, *Philip Morris Brands Sarl v Secretary of State for Health,* ECLI:EU:C:2016:32. On the broadness of Art. 114 functional limitations see also Gareth T Davies, 'The Competence to Create an Internal Market: Conceptual Poverty and Unbalanced Interests' in Sacha Garben and Inge Govaere (eds), *The Division of Competences between the EU and the Member States: Reflections on the Past, the Present and the Future* (Hart Publishing 2017) 75–76.

growing relevance of national security and technological sovereignty matters in cybersecurity policy – which is especially evident at Member States level,[35] for national security remains the sole responsibility of each Member State[36] – complicates the issue of EU competence even further.[37]

As anticipated in the introduction, from the adoption of the NIS Directive in 2016, the legal basis of EU cybersecurity legislation has been Article 114 TFUE, on the functioning of the internal market. Lacking a clear legal basis in the Treaties, the Commission carefully established, from early 2000s, a direct connection between the Single Market and cybersecurity,[38] through various Communications[39] and Strategies,[40] that eventually led to legislation, such as the NIS and NIS2 Directive and the Cybersecurity Act.

Essentially, the problem boils down to over-stretching the market justification to accommodate the multi-faceted issues tackled by EU cybersecurity policy – which only in part relates to the functioning of the Single Market and increasingly intertwined with individual safety and fundamental rights. In the IoT era, limiting the concept of 'cybersecurity' to just the protection of networks, information systems and information is too restrictive and ultimately anachronistic. Cybersecurity is ever more crucial to upholding *fundamental* values, such as fundamental rights and liberties, and physical safety.

Introducing a fundamental right to cybersecurity in EU law would thus support individuals' expectation to enjoy a secure digital life and, subordinately, it may grant EU secondary legislation an autonomous legal basis, thereby following a similar path of EU data protection law. Whereas the Data Protection Directive of 1995 relied on the internal market legal basis, the General Data Protection Regulation finds its legal basis in the protection of the right to data protection. Amending the EU Charter of Fundamental Rights pursuant to the procedure set out in Article 48 would not be enough though. Thus, Art. 6(1) TEU clearly states that "the provisions of the Charter shall not extend in any way the competences of the Union as defined in the Treaties". Fundamental rights, and Article 8 of the Charter makes no exception,[41] indeed do not establish competences "but are concerned with their exercise and therefore presuppose them".[42]

Experience in the field of data protection law can assist again.[43] Art. 16 of the TFEU enunciates, in its first paragraph, the right to data protection ("everyone has the right to the protection of personal data concerning them") – covered as well by the EU CFR at Art. 8 – and, in the second paragraph, explicitly sets out EU mandate to regulate the field of data protection as established by the Treaty :[44] "the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union". The EU co-legislators could enact the GDPR to protect the right to data protection exactly because Art. 16(2) TFEU granted them the power to do so.[45]

A Treaty modification, however intricate this might be,[46] appears therefore necessary to protect cybersecurity on the highest level, notwithstanding any allegedly 'parent right'[47] in the off-line sphere, and to give EU mandate to regulate a field which is progressively at odds with the only internal market legal basis.

3. The content of a new fundamental right to cybersecurity

After concluding that acknowledging a new fundamental right to cybersecurity should be the next step for EU policy makers, this section focuses on the content of such a new right. In particular, it shall be explored whether its formulation should hinge on a traditional human rights approach by means of declaration or, rather, prescriptive by including positive or negative obligations (or both) and for which addresses (i.e., only public actors and private entities or possibly even society at large).

In this endeavour, the European Declaration on Digital Rights and Principles for the Digital Decade (hereinafter, the Declaration)[48] could serve as an inspiration *par excellence* in shaping the actual content of a new fundamental right to cybersecurity. The Declaration consists of six Chapters[49] and twenty-four high level principles, inspired by the traditional fundamental rights style approach. Interestingly, these principles are accompanied by several political intentions or commitments by EU

[35] Sandra Schmitz-berndt and Pier Giorgio Chiara, 'One Step Ahead: Mapping the Italian and German Cybersecurity Laws against the Proposal for a NIS2 Directive' [2022] International Cybersecurity Law Review.

[36] Treaty on the European Union, Art. 4(2); see also Council of the EU, "Council Conclusions on exploring the potential of the Joint Cyber Unit initiative" 12534/21 (2021) <https://data.consilium.europa.eu/doc/document/ST-12534-2021-INIT/en/pdf> accessed 26 July 2023, 5.

[37] Marton Varju, '5G Networks, (Cyber)Security Harmonisation and the Internal Market: The Limits of Article 114 TFEU' (2020) 4 European Law Review 471.

[38] Brandão and Camisão (n 11) 1350; Annegret Bendiek and Eva Pander Maat, 'The EU's Regulatory Approach to Cyber-Security' (2019) 27 <https://www.swp-berlin.org/publications/products/arbeitspapiere/WP_Bendiek_Pander_Maat_EU_Approach_Cybersecurity.pdf> accessed 24 July 2023.

[39] European Commission, "Network and Information Security: Proposal for A European Policy Approach", COM(2001) 298 final 2.

[40] European Commission and the High Representative of the Union for Foreign Affairs and Security Policy (n 9) 5; European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", JOIN(2017) 450 final 3; European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, "The EU's Cybersecurity Strategy for the Digital Decade", JOIN(2020) 18 final 5.

[41] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, vol 16 (Springer International Publishing 2014) 166; Bart van der Sloot, 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right?' in Ronald Leenes and others (eds), *Data protection and privacy: (in)visibilities and infrastructures* (Springer 2017) 12–19.

[42] Tobias Lock, 'Article 6 TEU' in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (Oxford Academic 2019) 82.

[43] On whether EU personal data protection and cybersecurity can be considered 'neighbouring fields' see: Papakonstantinou (n 5) 13–14; Alessandro Mantelero and others, 'The Common EU Approach to Personal Data and Cybersecurity Regulation' (2021) 28 International Journal of Law and Information Technology 297.

[44] van der Sloot (n 41) 11.

[45] Regulation (EU) 2016/679, recital 12.

[46] András Jakab and Lando Kirchmair, 'Two Ways of Completing the European Fundamental Rights Union: Amendment to vs. Reinterpretation of Article 51 of the EU Charter of Fundamental Rights' (2022) 23 Cambridge Yearbook of European Legal Studies 1, 11; Carlos Closa, *The Politics of Ratification of EU Treaties* (Routledge 2018).

[47] Dror-Shpoliansky and Shany (n 23) 1256.

[48] Joint Declaration of the European Parliament, the Council and the European Commission, European Declaration on Digital Rights and Principles for the Digital Decade (2023/C 23/01).

[49] The Chapters of the Declaration are: I) Putting people at the center of the digital transformation; II) solidarity and inclusion; III) Freedom of choice; IV) Participation in the digital public space; V) Safety, security and empowerment; VI) Sustainability.

co-legislators. According to digital constitutionalism scholars, the Declaration is part of a broader picture whereby future EU digital policy will be based on a compass[50] underpinned by EU (digital and constitutional) values.[51]

Notably, the main political goal of the Declaration is stating that EU values and fundamental rights are equally applicable offline and in the digital environment: "the digital transformation should not entail the regression of rights. What is illegal offline, is illegal online".[52] This latter point, recalling inter alia the principle underlying the Digital Services Act,[53] explicitly recognises how relevant the digital sphere is nowadays in the life of citizens and implicitly confirms how blurring the boundaries between 'online' and 'offline' dimensions are, as seen in Section 2.1.

It has been noted that the Declaration "does show a willingness on the part of EU policymakers to accede the conversation on new digital rights".[54] On the other hand, the Declaration is not legally binding for Member States or private actors, nor does it grant any new enforceable right to EU citizens, nor does it affect the content of legal rules or their application.

From a constitutional perspective, the Declaration *per se* does not bring about alterations to the current EU framework, for it has declaratory nature. At the same time, as rightly noted by De Gregorio, "it cannot be excluded that courts, particularly the European Court of Justice, will refer to this instrument as a creative source of constitutional interpretation of the Charter, also considering the judicial activism shown by the CJEU in these years".[55]

For the purpose of this article, we shall focus on the 16th principle, concerning a 'protected, safe and secure digital environment'. It recites as follows:

> *"Everyone should have access to digital technologies, products and services that are by design safe, secure, and privacy-protective, resulting in a high level of confidentiality, integrity, availability and authenticity of the information processed"*.[56]

Moreover, the Declaration spells out three political intentions that ought to guide policy makers when implementing this principle:

> "a) taking further measures to promote the traceability of products and make sure only *products which are safe and compliant with EU legislation are offered* on the Digital Single Market [emphasis added];
> b) protecting the interests of people, businesses and public institutions against cybersecurity risks and cybercrime including data breaches and identity theft or manipulation. *This includes cybersecurity requirements for connected products* placed on the single market [emphasis added];
> c) countering and holding accountable those that seek to undermine, within the EU, security online and the integrity of the digital environment or that promote violence and hatred through digital means".[57]

The 16th principle of the Declaration may be used as an inspiration to lay down the normative groundwork for a new right to cybersecurity, albeit with some caveats. While it is declaratory in nature ('everyone should have access to digital technologies…'), the list of commitments that follow is rather prescriptive and already sheds light on addressees and recipients. Commitments a) and b) clearly hinge on typical EU product-safety terms, thereby foreseeing safety- and cybersecurity-related (essential) requirements for those economic operators who intend to place products on the Single Market.[58]

However, while recipients of this principle are not only the people – also in their vest of consumers of digital products, but also 'business and public institutions' potentially affected by cybersecurity risks, recipients of a new right to cybersecurity shall solely be individuals. The Declaration's holistic approach aligns with the Cybersecurity Act's broad understanding of cybersecurity whereby also '*other persons affected by cyber threats*' shall be in scope of cybersecurity activities. If 'a duty of care' on behalf of the economic operators involved – albeit to different degrees – in the value chain of digital products can be found in the text, there is regrettably no mention of any 'cyber-hygiene'[59] practice to be taken by individuals.

In terms of the subject-matter and scope, the legal interest safeguarded by the principle is the access to safe, secure and privacy-protective digital technologies, that is, products and services. However, a new fundamental right to cybersecurity shall not *directly* cover the technological assets used by individuals nor it should serve another right i.e., the fundamental right to privacy; instead, following the declaratory approach of the 16th principle, it should ensure that individuals can enjoy a 'secure digital life', leaving to secondary law how to implement this right through appropriate and proportionate regulatory measures.

In this respect, to protect this collective interest against cybersecurity risks, including – but not limited to cybercrime, the principle envisages, one the one hand, measures to enhance the resilience of digital technologies and products and, on the other hand, rules to holding accountable those that seek to undermine security online and the integrity of the digital environment. It follows that an internal balancing, similar to what happened in EU data protection law,[60] might be required. All in all, the policy benchmarks that particularise the principle seems comprehensive enough in terms of the challenges that a right to cybersecurity will face.

From a comparative perspective, EU legislature could also use as a benchmark digital bill of rights already proposed at Member States level.

[50] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 2030 Digital Compass: the European way for the Digital Decade' COM/2021/118 final; Decision (EU) 2022/2481 establishing the Digital Decade Policy Programme 2030 COM/2021/574 final.

[51] Giovanni De Gregorio, 'The Declaration on European Digital Rights and Principles: A First Analysis from Digital Constitutionalism' (The Digital Constitutionalist, 02 February 2022) <https://digi-con.org/the-declaration-on-european-digital-rights-and-principles-a-first-analysis-from-digital-constitutionalism/> accessed 24 July 2023.

[52] EU Declaration on Digital Rights and Principles, recital 3.

[53] Council of the EU, "What is illegal offline should be illegal online: Council agrees position on the Digital Services Act" <https://www.consilium.europa.eu/en/press/press-releases/2021/11/25/what-is-illegal-offline-should-be-illegal-online-council-agrees-on-position-on-the-digital-services-act/> accessed 26 July 2023.

[54] Cocito and De Hert (n 24) 9.

[55] Giovanni De Gregorio (n 51).

[56] EU Declaration on Digital Rights and Principles, point 16.

[57] *Ibidem.*

[58] As rightly noted by Cocito and De Hert (n 24) 11, the Declaration's use of market-friendly terms, which substantially differ from human rights tradition and language, is due to the fact that the Commission's department tasked to draft the document was the Directorate for Communication Networks, "entitled as it is to develop the digital single market, not fundamental rights".

[59] Mariarosaria Taddeo, 'Is Cybersecurity a Public Good?' (2019) 29 Minds and Machines 349, 352; Lorenzo Pupillo, 'EU Cybersecurity and the Paradox of Progress ' (2018) 6–7 <https://www.ceps.eu/ceps-publications/eu-cybersecurity-and-paradox-progress/> accessed 5 October 2021.

[60] Gloria González Fuster and Raphaël Gellert, 'The Fundamental Right of Data Protection in the European Union: In Search of an Uncharted Right' (2012) 26 International Review of Law, Computers and Technology 73, 77; cfr. with Opinion of Advocate-General Ruiz Jarabo Colomer, delivered on 22 December 2008 for Case C-553/07, *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer* § 25.

Italy and Spain, for example, acknowledged amongst new digital rights 'security in the web'[61] and 'a right to cybersecurity'[62] respectively. Spain spells out this new right far more boldly than Italy, as testified inter alia by the article's heading, albeit it unduly restricts the scope on (digital) information systems without putting individuals at the center.

In particular, the first paragraph of this right appears to be similar in essence with the principle of the EU Declaration. The additional element in the Spanish wording is represented by a twofold explicit positive obligation for (national) public authorities: i) they must enforce the right by ensuring that digital systems are adequately secure; ii) they have to promote cybersecurity awareness and training for society at large. This latter point is to be welcomed and aligns with Art. 7(1)(h) of Directive (EU) 2022/2555 (NIS2) which requires Member States to detail in their national cybersecurity strategy a plan, including necessary measures, to enhance the general level of cybersecurity awareness among citizens.

To conclude the second part of our analysis, notwithstanding the political and legal hurdles that are present on the path towards the recognition of such a right, the 'seeds' of a new fundamental right to cybersecurity in EU law already peak out above both EU's and Member States' ground.

4. Implementing the right to cybersecurity

After having explored the possible subject-matter, scope, recipients and addresses of a new fundamental right to cybersecurity, the legal analysis should address the legal measures through which such right could be implemented. At present stage, such new right may find legislative expression in the Commission's proposal for a Cyber Resilience Act (CRA) insofar product security is concerned.[63] In terms, on the other hand, of services' cybersecurity requirements, the EU legislative framework is more mature: Directive (EU) 2022/2555 (NIS2) will regulate vast majority of digital services in the EU from a cybersecurity standpoint.[64]

Albeit issues of liability fall outside the scope of the present paper, some preliminary remarks are nonetheless in place. The CRA proposal does not afford any remedy to individuals in case EU cybersecurity law's addresses infringe their obligations, contrary to the expectations of different stakeholders, including EU consumer association BEUC.[65] In the same vein, the other legal acts in EU cybersecurity law i.e., the NIS Directive, the new NIS2 Directive and the Cybersecurity Act do not afford any rights nor remedies to individuals, as they address the security of network and information systems and the EU cybersecurity certification framework respectively.[66] These legal acts have thus their primary objectives in the 'functioning of the internal market' and not the protection of natural and/or legal persons *per se*.

If we were to seek means of redress in the CRA, we would be disappointed. Aside from resorting to the traditional national liability schemes, a solution to the seemingly liability conundrum may come from another legal instrument. In this regard, it should be worth exploring the synergies between the CRA and the newly proposed Directive on liability for defective products[67] for it will deem a product to be defective when it does not provide inter alia safety-relevant cybersecurity requirements which the public at large is entitled to expect.[68] These cybersecurity requirements are laid down in the CRA[69] and – where the CRA does not apply – in the General Product Safety Regulation[70] or in other sectoral legislation.[71] In other words, the revision of the legal framework on liability for defective products will eventually provide individuals with means of redress if a cybersecurity vulnerability of a product is exploited and, accordingly, damages occur.

4.1. Implementing the right to cybersecurity: secure products

The proposed Cyber Resilience Act would complement EU cybersecurity *acquis* which appears to be fragmented vis-à-vis products' cybersecurity.[72] For it would lay down horizontal cybersecurity requirements for all products with digital elements, thereby implementing both the commitments a) and b) underpinning the principle 16 of the Declaration.

In particular, the CRA proposal applies "to products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network".[73] Importantly, the proposal gives a rather broad understanding of 'products with digital elements' i.e., "any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately".[74] The large scope of the CRA would thus implement a new right to cybersecurity insofar it aims at ensuring access to safe and secure "digital technologies and products".

Without dwelling on the merit of the Cyber Resilience Act too extensively, an overview over the main pillars of the Commission's proposal is nonetheless necessary. This legislative initiative builds upon the New Legislative Framework (NLF) structure and principles. The NLF

[61] Dichiarazione dei diritti in Internet (2015), Art. 13: "security on the Web shall be ensured as a public interest, through the integrity of infrastructures and their protection from attacks, and as an interest of individuals. Restrictions on freedom of thought are not permitted. The protection of people's dignity against abuses related to behaviour such as incitement to hatred, discrimination and violence must be guaranteed [translated by the author]".

[62] Carta Derechos Digitales (2021), Art. 6: "everyone has the right to ensure that the digital information systems they use for their personal, professional or social activity, or which process their data or provide them with services, have adequate security measures in place to guarantee the integrity, confidentiality, availability, resilience and authenticity of the information processed and the availability of the services provided. Public authorities, in accordance with European and national rules, shall ensure that the guarantees expressed in the previous paragraph are met by all information systems, whether publicly or privately owned, in proportion to the risks to which they are exposed. To this end, they may count on the collaboration of civil society. Public authorities shall promote cybersecurity awareness and training for the whole of society and promote certification mechanisms [translated by the author]".

[63] European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM(2022) 454 final.

[64] Even if the NIS2 is already into force, it is not applicable yet.

[65] BEUC, 'Cyber Resilience Act: Cybersecurity of Digital Products and Ancillary Services - BEUC Response to Public Consultation' (2022) 12 <https://www.beuc.eu/publications/beuc-x-2022-051_cyber_resilience_act_public_consultation_beuc_position_paper.pdf>.

[66] Papakonstantinou (n 5) 9–11.

[67] Proposal for a Directive of the European Parliament and of the Council on liability for defective products.

[68] Directive on liability for defective products proposal, Art. 6(1)(f).

[69] Cyber Resilience Act proposal, recital 16.

[70] Regulation (EU) 2023/988, Art. 6(1)(g), recital 26.

[71] Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC.

[72] Pier Giorgio Chiara, 'The Cyber Resilience Act: The EU Commission's Proposal for a Horizontal Regulation on Cybersecurity for Products with Digital Elements' (2022) 3 International Cybersecurity Law Review 255.

[73] Cyber Resilience Act proposal, Art. 2(1).

[74] Cyber Resilience Act proposal, Art. 3(1). With regard to software in particular, recital 9 of the CRA Proposal specifies that Software-as-a-Service (SaaS) falls outside of scope, "except for remote data processing solutions relating to a product […] for which the software is designed and developed by the manufacturer of the product concerned or under the responsibility of that manufacturer, and the absence of which would prevent such a product with digital elements from performing one of its functions".

reformed the internal market for goods by strengthening the conditions for making available a wide range of products on the internal market.[75] Against the backdrop of the market-oriented commitments of letters a) and b) of point 16 of the Declaration (see above), the choice of such legislative technique seems appropriate to meet the political goals underpinning the cybersecurity principle enshrined in the Declaration.

Products with digital elements can be made available on the single market under two main conditions :[76] i) they meet the essential requirements set out in Section 1 of Annex I, relating to the properties of products ;[77] and, ii) the processes put in place by the manufacturer in terms of vulnerability handling comply with the essential requirements set out in Section 2 of Annex I.[78]

The CRA proposal hinges on a risk-based approach: among the various obligations, manufacturers must perform an assessment of the cybersecurity risks associated with a product, the outcome of which shall be taken into account in all the phases of the product's life-cycle (from planning and design to delivery and maintenance) with a view to minimising cybersecurity risks, preventing security incidents and minimising the impacts of such incidents, including in relation to the health and safety of users.[79] This provision explicitly links digital and the physical dimension, by mentioning potential impacts on individual safety. The argument previously made regarding the instrumental value that cybersecurity bears on safety (and other fundamental values too) holds.

In line with the risk-based character of the proposal, specific categories of products with digital elements can be classified as critical[80] or highly critical[81] reflecting the level of cybersecurity risk related to such products. The difference between non-critical, critical and highly critical products primarily rests with the different conformity assessment procedure they must undergo amongst the list of Annex VI. The CE marking must be affixed visibly, legibly and indelibly to the product with digital elements before it is made available on the market.[82]

National market surveillance authorities (MSAs) —designated by Member States—carry out market surveillance in the territory of that Member State. In terms of enforcement, MSAs may conduct control actions[83] and require operators to take all appropriate corrective measures to bring the product into compliance with CRA requirements, to withdraw it or to recall it from the market (Art. 43). Rules on administrative fines are decided by Member States but CRA proposal limits States discretion by adopting a GDPR-alike scalable approach to penalties (Art. 53).

Notwithstanding its anchoring in product safety legislation,[84] and bearing in mind the products security-related political commitments of the Declaration, the Cyber Resilience Act seems to be fit for enforcing a right to cybersecurity for it will ensure more cybersecure products for individuals in the EU.

4.2. *Implementing the right to cybersecurity: secure services*

On 27 December 2022, Directive (EU) 2022/2555 (hereinafter, NIS2) was published in the Official Journal of the EU and entered into force on 16 January 2023. Yet, on the same day, two other important pieces of legislation have been published in the EU OJ, namely Directive (EU) 2022/2557 on the resilience of critical entities (CER directive) and Regulation (EU) 2022/2554 on the digital operational resilience of financial entities (DORA regulation). Whereas the former hinges on entities physical security[85] – and thus not cybersecurity – the latter shall be considered sector-specific (banking and finance sector) and thus *lex specialis* in relation to the NIS2.[86]

The NIS2 seeks to modernise the existing legal framework and addresses several weaknesses that prevented the existing Directive from unlocking its full potential. The explanatory memorandum of the Proposal for the NIS 2 acknowledged that the NIS Directive had contributed to enhance the overall level of cybersecurity in EU.[87] However, the evaluation on the functioning of the NIS Directive highlighted several limitations.[88]

For the purposes of this article, this section concentrates on four structural changes brought about by the NIS2 to the NIS framework, to highlight to what extent the NIS2 contributes to more cyber-secure

[75] The New Legislative Framework consist of Regulation EU 765/2008; Decision 768/2008; Regulation EU 2019/1020 (the latter being amended by the CRA), see European Commission (2016) "The 'Blue Guide' on the implementation of EU products rules 2016 (2016/C 272/01)" Off. J. Eur. Union. In a nutshell, harmonised legislation limits to laying down the essential requirements (ERs) that products made available on the EU market must meet. These ERs are then specified by harmonised technical standards drafted by European Standardisation Organisations (ESOs, i.e. ETSI, CEN, CENELEC) on the basis of a standardisation request by the Commission: if products comply with these standards, they benefit from a presumption of conformity with the corresponding ERs. Thus, the NLF envisages different conformity assessment modules according to which manufacturers demonstrate whether ERs relating to a product have been fulfilled. National market surveillance authorities are tasked to take appropriate measures to prevent the making available on the market and use of non-compliant products.

[76] Cyber Resilience Act proposal, Art. 5.

[77] There are two main ERs: products with digital elements i) shall be designed, developed and produced to ensure an appropriate level of cybersecurity based on the risks; ii) shall be delivered without any known exploitable vulnerabilities. Other essential requirements include: secure by default configuration; protection from unauthorised access through appropriate control mechanisms; protection of the confidentiality of processed personal or other data by means of state-of-the-art encryption, etc.

[78] These ERs include: identification and documentation of vulnerabilities and components contained in the product, including a software bill of materials (SBOM) in a machine-readable format covering at least products' top-level dependencies; mitigation of vulnerabilities without delay, by providing security updates; application of effective and regular tests and reviews of products' security; public disclosure of information about fixed vulnerabilities, etc.

[79] Cyber Resilience Act proposal, Art. 10(2). Manufacturers also have documentation obligations in terms of technical documentation (Art. 23; Annex V) and reporting obligations (Art. 11). Manufacturers draw up the EU declaration of conformity as part of the documentation duties (Art. 10(7)), stating that compliance with Annex I's ERs has been fulfilled.

[80] Annex III, Cyber Resilience Act proposal. There are two classes of critical products (class I and II), according to the level of cybersecurity risk related to a specific category.

[81] Commission is empowered to specify through delegated acts which categories of products shall be considered as 'highly critical' and thus required to obtain a European cybersecurity certificate under a scheme pursuant to Regulation (EU) 2019/881 to demonstrate conformity with the essential requirements.

[82] Cyber Resilience Act proposal, Art. 22(1).

[83] Potentially involving other MSAs through joint coordinated activities as per Arts. 48 and 49.

[84] Chiara (n 72) 262–263.

[85] Directive (EU) 2022/2555, recital 30.

[86] Directive (EU) 2022/2555, recital 28.

[87] European 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 COM (2020) 823 Final' (2020) <https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF> accessed 3 August 2023.

[88] ibid 5. Areas of concern were: i) the limited scope in terms of sectors covered; ii) unclear rules regarding the identification of operators of essential services; iii) wide discretion to Member States when deciding security and incident reporting requirements; iv) ineffective supervision and enforcement regime; v) lack of cooperation and information sharing.

services for individuals in the EU. To this end, the analysis synthetically casts light on i) the wider scope of the NIS2; ii) revised cybersecurity risk-management measures and reporting obligations for NIS2 entities; iii) rules on cybersecurity information sharing and vulnerability disclosure; and iv) supervisory and enforcement framework.

The NIS Directive has proved to fail in reflecting all digitised sectors that provide key services in the Union. As a consequence, the scope of the NIS2 has been extended to comprehensively cover those sectors and services that are of vital importance to societal and economics activities. The obsolete distinction between operator of essential services (OESs) and digital service providers (DSPs) is thus replaced by essential entities (EEs) and important entities (IEs), reflecting the extent to which they operate in a critical sector, or they provide a certain service. To overcome divergences among Member States in terms of OESs identification which was based on national criteria, Article 2 NIS2 lays down a size-cap rule across the Union: public and private entities covered in Annex I (sectors of high criticality)[89] and II (other critical sectors)[90] which are at least medium-sized enterprises fall in scope of the Directive. However, there are some exceptions for which the Directive applies to entities regardless of their size.[91]

While the NIS Directive had already introduced security measures and incident reporting duties for OESs and DSPs, Member States were allowed wide discretion when laying down such requirements for OESs. To harmonise an otherwise fragmented framework, the NIS2 sets out a list of minimum cybersecurity measures that both EEs and IEs must adopt, following a risk-based approach,[92] and strengthens incident reporting duties, again without differentiating between EEs and IEs. The measures that entities have to implement to manage the risks posed to their NIS include, among others: risk analysis and information system security policies; incident handling; business continuity and crisis management; supply chain security; etc.[93] In terms of reporting obligations, Art. 23 NIS2 foresee a more stringent and detailed timeframe,[94] subsequent steps for notifying the competent authority[95] and a widening of the notion of 'significant incident' triggering the notification duty.[96]

To enhance EU's cybersecurity situational awareness and the overall level of cyber resilience and security, the NIS2 importantly introduces at Art. 12 rules on vulnerability handling and disclosure and at Art. 29 a framework on voluntary information sharing arrangements. As regards the former, each national CSIRT acts as a trusted intermediary, facilitating the interaction between the party reporting a vulnerability and the manufacturer or provider of the vulnerable ICT products or services. ENISA, on the other hand, is tasked to develop and update a "European Vulnerability Register", containing a description of the vulnerability, including its severity, the assets concerned, the availability of related patches and, if not available, guidance on how to mitigate the risks.[97] Having regard to voluntary information-sharing, Member States shall ensure that entities wanting to exchange relevant cybersecurity information (e.g., cyber threats, near misses, vulnerabilities, techniques and procedure, etc.) with other EEs and IEs can do so through arrangements taking into account the sensitive nature of the shared data.

Provided that the NIS Directive's enforcement regime had proved to be ineffective, the NIS2 strengthens national competent authorities' powers and tasks. Supervisory and enforcement measures are now more detailed (e.g., on-site inspections, targeted security audits, security scans, requests for information and to access data, etc.) but are differentiated depending on whether the authority enforces them against an EE or an IE, the latter being subjected to *ex-post* supervisory measures.[98] In terms of penalties, mirroring the sanctioning model of Article 83(4) GDPR, Art. 34 NIS2 lays down severe administrative fines of up to €10 M or 2 % of the total worldwide annual turnover (whichever is higher) of the undertaking for infringements of cybersecurity risk management and reporting obligations.

The above overview on some of the major impacts brought by the NIS2 on the EU market of services served to show how this legal act considerably strengthens the level of protection offered by the NIS Directive.[99] Many new market players will fall in scope of the new NIS2. As a result, they will have to increase their cybersecurity posture, which in turn would result in mitigating potential loss due to incidents. For citizens, more cyber resilient and secure services would result in reduced material (i.e., loss of income) or non-material damages. Therefore, the NIS2 seems to be fit for enforcing a new right to cybersecurity insofar a safe and secure access to services is considered.

5. Conclusion

A new right to cybersecurity would best protect individuals in their increasingly digital (on-)life. Furthermore, it may also guide the fast-growing regulatory landscape and support the emergence of the new policy field of EU cybersecurity law.[100] As of now, EU lacks explicit competence to legislate in the cybersecurity field. EU cybersecurity law, which primarily has been enacted on the internal market legal basis under Art. 114 TFUE, shifted relatively recently, that is, from the adoption of the Cybersecurity Act in 2019, from organisational and technical legislation to a comprehensive multi-level and multi-stakeholder regulatory approach.[101]

Recent initiatives both at political and legislative level show that cybersecurity pose legal challenges going far beyond obstacles to the Single Market. Related to that, cybersecurity in EU is increasingly seen as a shared responsibility between the public sector, which has to provide the relevant legal frameworks, the private sector, which has to design and place in the market products with effective cybersecurity and users of digital technologies, who also have a role to play vis-à-vis a

[89] The sectors are: energy; transport; banking; financial market infrastructures; health; drinking water; waste water; digital infrastructure; ICT service management; public administration; space.

[90] The sectors are: postal and courier services; waste management; manufacture, production and distribution of chemicals; production, processing and distribution of food; manufacturing; digital providers; research.

[91] Directive (EU) 2022/2555, Art. 2(2); (3); (4).

[92] Directive (EU) 2022/2555, Art. 21(1), recital 82.

[93] Directive (EU) 2022/2555, Art. 21(2).

[94] Whereas the NIS Directive enforced the so-called "without undue delay" standard without specific timeframe, the NIS2 requires entities to submit competent authorities an early warning within 24 hours of becoming aware of the significant incident and a more complete notification within 72 hours.

[95] The single notification of the previous directive is 'split' into several stages: an early warning, the actual incident notification, an intermediate report – if requested by the competent authority - and a final report.

[96] Directive (EU) 2022/2555, Art. 23(3): an incident shall be considered 'significant' if a) has caused/capable of causing severe operational disruption of the services or financial loss for the entity; b) has affected/capable of affecting natural or legal persons by causing considerable material or non-material damage.

[97] Directive (EU) 2022/2555, Art. 12(2).

[98] Directive (EU) 2022/2555, Art. 33.

[99] Pier Giorgio Chiara, 'The IoT and the New EU Cybersecurity Regulatory Landscape' (2022) 36 International Review of Law, Computers & Technology 118, 14.

[100] Ramses A Wessel, 'Towards EU Cybersecurity Law: Regulating a New Policy Field' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing Ltd 2015).

[101] European Commission and the High Representatitve of the Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade' (2020) 23.

more secure digital environment through the adoption of cyber-hygiene practices.[102]

Acknowledging such right into EU law is not straightforward. However, this article contributed to show that the basic components of such new right are in place, EU having already taken concrete steps towards this direction by laying down the normative groundwork for a new right to cybersecurity in the Declaration on Digital Rights and Principles for the Digital Decade. If introduced at some point in EU primary and secondary law, this new fundamental right should reflect the *holistic* and declaratory approach of the Declaration.

In terms of the scope, holistic approach means that access to digital technologies should be ensured in a safe and (cyber)secure way. Recipients therefore should include *every natural person.* In turn, addresses would be those actors that actually play a role in ensuring a secure and safe access to digital technologies serving individuals. This includes public and private entities, already designated in EU cybersecurity legislation, having the power to protect people against cybersecurity risks but also those who seek to undermine, within the EU, security online and the integrity of the digital environment.

As a consequence, individuals would be afforded with legal means to protect their interest to enjoy a safe and secure digital life. Against this backdrop, the Cyber Resilience Act, on the one hand, and the NIS2 (and other sectoral legislation, such as the DORA Regulation) represent already a good starting point to operationalise such new fundamental right. In case a new right to cybersecurity is introduced in EU law later than the entry into force of the Cyber Resilience Act, the CRA (and also the NIS2) could be retroactively read as an interpretation of the right to cybersecurity, just as the European Court of Justice did vis-à-vis the 95′ Data Protection Directive and the fundamental right to data protection.[103]

Declaration of competing interest

The author declares that he has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgments

This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union – NextGenerationEU.

[102] Taddeo (n 59); Raffaella Brighi and Pier Giorgio Chiara, 'La Cybersecurity Come Bene Pubblico: Alcune Riflessioni Normative a Partire Dai Recenti Sviluppi Nel Diritto Dell'Unione Europea' (2021) 21 Federalismi.it 18.

[103] Fuster and Gellert (n 60) 78; van der Sloot (n 41) 11. Cfr. with CJEU Case C-543/09, *Deutsche Telekom AG v Bundesrepublik Deutschland,* ECLI:EU:C:2011:279 §50.