This is the final manuscript for academic use only. Please do not circulate without the author's permission, and always refer to the published version:

M. G. Porcedda, Patching the patchwork: appraising the EU regulatory framework on cyber security breaches, *Computer Law and Security Review* (CLSR), 2018, Vol. 34 (5), ISSN: 0267-3649.

Patching the patchwork: appraising the EU regulatory framework on cyber security breaches

ABSTRACT

Breaches of security, a.k.a. security and data breaches, are on the rise, one of the reasons being the well-known lack of incentives to secure services and their underlying technologies, such as cloud computing. In this article, I question whether the patchwork of six EU instruments addressing breaches (Framework Directive, e-Privacy Directive, eIDAS Regulation, PSD2, GDPR, NIS Directive) is helping to prevent or mitigate breaches as intended. At a lower level of abstraction, the question concerns appraising the success of each instrument separately. At a higher level of abstraction, since all laws converge on the objective of network and information security – one of the three pillars of the EU cyber security policy – the question is whether the legal 'patchwork' is helping to 'patch' the underlying insecurity of network and information systems thus contributing to cyber security. To answer the research question, I look at the regulatory framework as a whole, from the perspective of network and information security and consequently I use the expression cyber security breaches. I appraise the regulatory patchwork by using the three goals of notification identified by the European Commission as a benchmark, enriched by policy documents, legal analysis, and academic literature on breaches legislation, and I elaborate my analysis by reasoning on the case of cloud computing. The analysis, which is frustrated by the lack of adequate data, shows that the regulatory framework on cyber security breaches may be failing to provide the necessary level of mutual learning on the functioning of security measures, awareness of both regulatory authorities and the public on how entities fare in protecting data (and the related network and information systems), and enforcing self-improvement of entities dealing with information and services. I conclude with some recommendations addressing the causes, rather than the symptoms, of network and information systems insecurity.

Keywords: Data breaches, security breaches, cyber security, data protection, network and information security, cloud computing, data security breaches, GDPR, NIS Directive, Telecom Framework, eIDAS, PSD 2

1. Introduction

News of public and private organizations being breached proliferate. While not all breaches of security are caused by cybercrime,[1] the term generally refers to the unauthorized access to network and information systems, which can lead to further cybercrimes, such as the 'exfiltration' of data, i.e. the creation of unauthorized copies for dissemination, sale, or for blackmailing through the information contained in such data. Breaches of security affecting personal data, usually referred to as 'data breaches', have on average increased in size in 2017,[2] and are almost a daily occurrence, so much so that it has become difficult to keep track of them. The security firm Gemalto[3] boldly suggests that the question is not whether one's network and information system will be breached or not, but rather when the breach will take place.

Such a bleak scenario may not fully reflect reality yet, but could provide an accurate description of the (near) future, if the root causes of security breaches remain unaddressed. A well-known root cause of breaches is the underinvestment in network and information security, which is often seen as a burden, rather than an asset.[4] Hence, in addition to attaching criminal liability to perpetrating, or aiding and abetting, data and security breaches, several jurisdictions,[5] including the EU, have opted for the imposition of legal obligations to protect one's systems and data. These have been coupled with the adoption of legal devices such as the notification of breaches to a supervisory authority and, possibly, to the (affected) public.

In its Impact Assessment accompanying the proposed General Data Protection Regulation (hereafter GDPR), the European Commission identified three advantages of notification. In detail, "breach notifications provide a systematic feedback about the actual risk and the actual weaknesses of existing security measures; they enable authorities and consumers to assess the relative capabilities of data controllers with respect to data security; they force data controllers to assess and understand their own situation regarding security measures".[6] I dub the three advantages of notification as 'mutual learning', 'public awareness' and 'self-improvement' respectively. However, notification is not without faults: Burdon and others submit that it is conceptually incoherent, because it tries to balance conflicting concepts, "namely the provision of effective consumer protection and the prioritisation of corporate compliance cost mitigation."[7] Instead of being included in one overarching instrument, provisions on the notification and mitigation of data and security breaches have been inserted in separate instruments. Hence, I refer to the ensemble of EU laws on security breaches, including data breaches, as a regulatory 'patchwork'.

In this article, I question whether the EU regulatory framework is helping to prevent or mitigate breaches of security as intended. At a lower level of abstraction, the question concerns

[1] Other causes include human error, system glitch and natural disasters: David Wall, 'Enemies within: Redefining the insider threat in organizational security policy' 26 Security Journal 107-124; Larry Ponemon, *2017 Cost of Data Breach Study. Global Overview* (2017).

[2] Ponemon (2017), *2017 Cost of Data Breach Study. Global Overview*.

[3] See at: http://breachlevelindex.com/data-breach-risk-assessment-calculator (last accessed on 19th December 2017). Some commentators go in the same direction, suggesting that the focus should be on harm reduction rather than prevention. Ioannis Agrafiotis and others, *Cyber Harm: Concepts, Taxonomy and Measurement* (Saïd Business School WP 2016-23, 2016).

[4] Ross Anderson and Tyler Moore, 'The Economics of Information Security' (2006) 314 Science 610-661; Mark Burdon, Bill Lane and Paul von Nessen, 'Data breach notification law in the EU and Australia - Where to now?' 28 Computer Law & Security Review 296-307.

[5] The first law was passed by the State of California. Burdon, Lane and von Nessen (2012), 'Data breach notification law in the EU and Australia e Where to now?'. See also at: https://iapp.org/news/a/eu-data-breach-notification-rule-the-key-elements/.

[6] European Commission, *Commission Staff Working Paper SEC(2012) 72 final. Impact Assessment Accompanying the General Data Protection Regulation* (2012), p. 100.

[7] Burdon, Lane and von Nessen (2012), 'Data breach notification law in the EU and Australia - Where to now?', p. 302.

appraising the success of each instrument separately – to the extent feasible with respect to the availability of data and state of implementation of the rules. At a higher level of abstraction, since, as I will demonstrate, all laws converge on the objective of network and information security (one of the three pillars of the EU cybersecurity policy[8]), the question is whether the legal 'patchwork' is helping to 'patch' the underlying insecurity of network and information systems – thus contributing to cybersecurity. To answer the research question, I will look at the regulatory framework as a whole, from the perspective of network and information security, rather than focussing on the distinction between personal/non-personal data. To refer to all breaches, I use the expression 'cyber security breaches'.[9]This is in agreement with the suggestion advanced by Burdon et al.[10] I appraise the regulatory patchwork by using the three goals of notification identified by the European Commission as a benchmark; I further enhanced them with policy documents, legal analysis, and academic literature on data and security breaches legislation,[11] to which I endeavour to contribute.

I begin by illustrating the EU regulatory patchwork on breaches of security, which is composed of six instruments emerged through three regulatory waves. I subsequently illustrate the 'state of the framework', by focussing in particular on the definition of breaches, the rules on the notification and mitigation of breaches, and provisions on inventories, sanctions and liabilities. In the next section, I appraise the regulatory framework. The only instruments that can be appraised individually and hence lead to answering the research question at a lower level of abstraction, are those relating to the first regulatory wave. Based on the (unsatisfactory) evidence gathered, I propose a method to evaluate the regulatory framework as a whole at the higher level of abstraction. I then reason on the implications of my findings with reference to the case of cloud computing, which is addressed in both the second and third regulatory wave. There, I propose to reflect on the possible consequences of the state of the art with reference to the scenario of universities with teaching hospitals. I must warn the reader that the analysis is speculative due to the evolving legal landscape. In the conclusion, I address the pun in the title, i.e. whether the legal patchwork 'patches' the insecurity of network and information systems causing breaches, and further fuelled by breaches, and whether it needs patching to do so.

[8] European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU* ((Joint Communication)JOIN(2017) 450 final, 2017); European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, *Cyber Security Strategy: An Open, Safe and Secure Cyberspace* ((Joint Communication) JOIN (2013) 01 final, 2013).

[9] The term cyber security breaches does not have legal significance, but, as I hope to illustrate in section 3, nicely captures the gist of the problem. It is currently used in the UK yearly official statistics on breaches (see at: https://www.gov.uk/government/collections/cyber- security- breaches- survey).

[10] Burdon, Lane and von Nessen (2012), 'Data breach notification law in the EU and Australia - Where to now?'

[11] Burdon, Lane and von Nessen (2012), 'Data breach notification law in the EU and Australia - Where to now?'; Apostolos Malatras and others, 'Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities' 33 Computer Law and Security Review 458-469; Rachel M. Peters, 'So You've Been Notified, Now What? The Problem with Current Data Breach Notification Laws' (4) 56 Arizona Law Review 1171-1202; Rosa Barcelo, 'EU: Revision of the ePrivacy Directive.' (2009) 31 Computer Law Review International 31; Rebecca Wong, *Data Security Breaches and Privacy in Europe* (Springer 2015).

2. The EU law on cyber security breaches: 3 regulatory waves, 2 regimes, seven addressees

There are at least eleven instruments of EU law having a bearing on breaches, five in the Area of Freedom, Security and Justice (AFSJ)[12] and six in the internal market.[13] This article concerns instruments that (mostly) find their legal basis in Article 114 of the Treaty on the Functioning of the European Union (TFEU, former Article 95, internal market), which were adopted in three waves, and are usually grouped into two different regimes, as I articulate in the following. Rules on breaches of security are covered in multiple instruments because the matter is mostly dealt with in a sectorial manner. There are at least seven different addressees, which I illustrate in the last section of this part.

2.1. THREE WAVES, TWO SEEMING REGIMES

Rules concerning breaches of security were introduced in three waves. The first wave occurred with the adoption of the so-called Telecom Package, composed of the Citizens' Rights Directive,[14] which amended the e-Privacy Directive, and the Better Regulation Directive[15] amending the Framework Directive. The former introduced in the e-Privacy Directive[16] rules on the prevention and mitigation of data breaches. The latter amended the Framework Directive[17] by adding rules on breaches of security.

The second regulatory wave includes four instruments, whose rules will enter into force in the course of 2018. The first is the Electronic Identification and Assurance Services (hereafter eIDAS) Regulation[18] (based on art. 294 TFEU), which contains provisions on breaches of security relating to

[12] Title V of the Treaty on the Functioning of the European Union, which deals with rapprochement of legislation in the area of criminal law, as well as police and judicial cooperation. Consolidated versions of the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU), OJ C 83/01 (Lisbon Treaty). Three are generic instruments that may be of use in case of computer crime-related investigations: the European Investigation Order Directive; the Proceeds of Crime Directive; and the European Arrest Warrant. The fourth AFSJ-related instruments is the Directive on attacks against information systems, which lays down substantive provisions on computer-related crimes to which data breaches usually refer. The fifth instrument is the Europol Regulation.

[13] I describe five of these instruments in detail in Maria Grazia Porcedda, 'Regulation of Data Breaches in the European Union: Private Companies in the Driver's Seat of Cybersecurity?' in Carrapico Helena and Olrdich Bures (eds), *Security Privatization How Non-security-related Private Businesses Shape Security Governance* (Springer 2018).

[14] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws, OJ L 337 (Citizens' Rights Directive).

[15] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, OJ L 337 (Better Regulation Directive).

[16] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, OJ L 201 (e-Privacy Directive).

[17] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a Common Regulatory Framework for Electronic Communications Networks and Services (Framework Directive), OJ L 108.

[18] Regulation 910/2014/EU of the European Parliament and Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC, OJ L257.

identity assurance services and trust services. The second is the reviewed Payment Services Directive (hereafter PSD2)[19] which introduced rules on operational and security incidents affecting in particular electronic payments enabled by payment services providers. The third is the Network and Information Security (hereafter NIS) Directive,[20] laying down rules on security incidents for the operators of essential services and digital service providers. The last instrument is the General Data Protection Regulation (hereafter GDPR),[21] originally based on both Arts. 114 and 16 TFEU (Art. 114 was eventually dropped, yet the GDPR fulfils the Digital Single Market), which includes wide-ranging provisions on data breaches.

The third regulatory wave, which is happening at the time of writing, concerns the overhaul of the Telecom Package. The European Electronic Communications Code (hereafter EECC)[22] updates the Framework Directive and broadens the addressees of such rules. In contrast, the proposed e-Privacy Regulation[23] (to be based, like the GDPR, on both Arts. 114 and 16 TFEU) is stripped off any norms on data breaches. This is because the GDPR is supposed to provide comprehensive and exhaustive legislation for all data breaches in this area, irrespective of the addressee.

The six internal market instruments tend to be conceptually grouped into two regimes. The e-Privacy Directive and the GDPR concern breaches affecting personal data, 'data breaches' for short. Their rationale is to create incentives of a legal and reputational nature that were hitherto missing so that entities processing personal data implement both security and privacy measures. The remaining four instruments concern 'incidents' or 'breaches of security' or 'loss of integrity' or 'security incidents' which do not necessarily affect personal data, and which are not always dealt with by means of creating incentives. However, as I will demonstrate in Section 3, the two regimes converge and, for the sake of averting breaches, they should be dealt with together, under the common label of 'cyber security breaches'.

2.2. ADDRESSEES *scope*

Multiple instruments cover rules on breaches because the matter is mostly dealt with in a sectorial manner. There are at least seven different addressees, though this does not immediately translate into seven clear-cut regimes of security breaches.

The e-Privacy and Framework Directives concern "electronic communications services", which are defined in article 2(c) of the Framework Directive.[24] 'Communications' is "any information

[19] Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337.

[20] Directive 2016/1148/EU of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union, OJ L 194.

[21] Regulation 2016/679/EU 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), OJ L 119/1. Note that the GDPR i the Digital Single Market.

[22] European Commission, *Proposal for a Directive Establishing the European Electronic Communications Code* ((Communication) COM(2016) 590 final, 2016/0288 (COD), 2016).

[23] European Commission, *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)* ((Communication) COM (2017) 10 final, 2017/0003(COD), 2017).

[24] "A service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information

exchanged or conveyed between a finite number of parties" (Art. 2 (d)). Broadcast communications (e.g. TV or radio) do not fall within this definition, unless "the information can be related to the identifiable subscriber or user receiving the information". Typically, communications by means of a publicly available electronic communication service would take place on a public communications network.[25] In brief, these rules apply to Telcos over electronic networks that are available to the public (i.e. not private), but concern neither content providers, nor Information Society Services, a category embracing many web-based businesses, as I will discuss further below. Note that, in the current draft, the EECC will also apply to e-mail providers.

The eIDAS Regulation concerns two categories: e-identification schemes notified by Member States, and trust service providers established in the Union, except those "used exclusively within closed systems resulting from national law or from agreements between a defined set of participants" (Art. 2). A trust service is an electronic service consisting of the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, and certificates for website authentication, as well as the preservation of electronic signatures, seals or certificates concerning those services (Art. 3 (16)). These are fundamental for e-government: by mid-2018, it will be mandatory to recognise mutually forms of e-identification across the Member States of the EU.[26] Trust services can be qualified or unqualified, and the latter can include commercial services.

The PSD2 addresses 'payment service providers', which engage in the business activities listed in Annex I. These include: traditional credit institutions, such as banks and building societies; electronic money institutions;[27] post office giro institutions; payment institutions, which include credit cards, money remittances and forex services;[28] and, under certain circumstances, the ECB, national central banks, as well as Member States and their regional entities (Art. 1 (a) to (e) and Recital 24). The Directive also covers payment institution services (PIS), which are third parties enabling online merchants to accept credit transfers,[29] and account information services (AIS), which aggregate financial information on the payer's behalf[30] (Art. 4 (3) and Annex I).

The NIS Directive also has two addressees, although they are broadly defined. The first are operators of essential services, i.e. public or private entities whose service: i) is 'essential for the maintenance of critical societal and/or economic activities'; ii) its provision 'depends on network and information systems'; and iii) would be highly disrupted by 'an incident' as seen above (arts. 4 (4) and 5 (1)). Annex II of the Directive contains a list of essential services, which are in the sectors of energy, transport, banking, financial market infrastructures, health, the drinking water supply and distribution, as well as digital infrastructure. The latter include Internet exchange points (IXPs), domain name system (DNS) service providers and Top Level Domain name registries, which can be exposed to breaches. The second addressees of the NIS Directive are three types of 'digital services', namely three types of (art. 4 (5)) Information Society Services offered in the EU (defined in section 4): search engines, online marketplaces and cloud computing. 'Online marketplace' are e-commerce

---

society services … which do not consist wholly or mainly in the conveyance of signals on electronic communications networks".

[25] Further discussed in Section 2.1.

[26] The website of DG Connect has a list of the qualified trust service providers (https://webgate.ec.europa.eu/tl-browser/#/) and the free e-signature package (https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/DSS).

[27] These deal with digital money. Examples of e-money providers can be found at: https://www.e-ma.org/our-members (last accessed on February 18th 2018).

[28] For a list of other services, see https://paymentinstitutions.eu/about-epif/the-payment-institutions-sector/about (last accessed on February 18th 2018).

[29] David Baker, *New Payment Initiation Service Providers & The Card Networks* (The London Institute of Banking and Finance 2017) <https://www.libf.ac.uk/news-and-insights/news/detail/2017/04/04/new-payment-initiation-service-providers-the-card-networks>.

[30] Editor, *FCA moves to clarify scope of regulation of account information services under PSD2* (Outlaw.com 2017).

services allowing purchasing of goods or services. Online search engines are the likes of Google, StartPage, or DuckDuckgo. 'Cloud computing services', which I will discuss in Section 5, include webmail services, platforms for the development of smartphone apps, and data servers and farms.

Finally, the GDPR is a horizontal instrument that will apply, broadly speaking, to any entity established in the Union that processes whosoever personal data, or to an entity not established in the Union that offers goods or services to data subjects in the Union. This includes the addressees of data breaches legislation described above,[31] such as digital services, as well as other Information Society Services, i.e. providers of content online.

3. Definition, goals, and tools of the EU regulatory framework on cyber security breaches

In this section, I compare and contrast the six instruments addressing cyber security breaches. First, I expound the different understandings of 'breach' contained in the legislation, and propose a common definition. Secondly, I revise the goals that the different instruments purport to pursue; while individual laws differ as to the final harm that they try to avert, they all share the overarching goal of achieving network and information security (understood as the first pillar of cybersecurity[32]). Thirdly, I illustrate the 'tools' commonly found in the three instruments to curb the occurrence of breaches: the adoption of technical and organisational measures, rules on notification of breaches and the timing thereof, and further instruments such as inventories, insurance, liability, burden of proof and sanctions.

as in integrity and confidentiality only, i.e. a sub-category of security incidents? Formally correct, but seems unlikely in practice. I. think of examples of loss of availability/authentication: these would lead to the outcome featured in the breach of security

3.1. DEFINITION OF BREACHES

Article 2 (h) (i) of the e-Privacy Directive defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"[33] ("in connection with the provision of a publicly available electronic communications service in the Community"). While this definition may not have been translated equally in the 28 national laws of the Member States (plus EFTA countries) transposing the Directive, nevertheless, as of 2018, it will apply uniformly throughout the EU thanks to the fact that the definition has been copied into the GDPR (Art. 4(12)).

Conversely, the Framework Directive does not define 'breach'. The notion is referred to in Article 13a(3), whereby "undertakings … notify the competent national regulatory authority of a breach of security or loss of integrity" affecting the operation of networks or service. Moreover, Article 13a(1) concerns "security incidents", which is also not defined.

Similarly, the eIDAS Regulation refers to "a breach of security or loss of integrity" (Recital 38 and Art. 17 (4)) impacting "on the trust service provided or on the personal data maintained therein" (Article 19 (2)), but does not define it. Also similarly to the Framework Directive, paragraph 1 of Art. 19 refers to 'security incidents' (see also Rec. 31). The same can be said for breaches "that affect…the cross-border authentication of that scheme" (Art. 10 (1)), whose meaning must be derived from the provision on notification in which they are mentioned. However, integrity is referred to in Article 3(5) of the Regulation, as a defining element of 'authentication', i.e. "an electronic process that enables the

[31] It should be noted that the only exception is represented by personal data processed by Telecoms, to whom the rules of the e-Privacy Directive apply for as long as the Directive will be in force.

[32] European Commission and High Representative of the European Union for Foreign Affairs and Security Policy (2013), *Cyber Security Strategy, JOIN (2013) 01 final*.

[33] For a discussion of the scope of the article, see Burdon, Lane and von Nessen (2012), 'Data breach notification law in the EU and Australia - Where to now?'; Wong (2015), *Data Security Breaches and Privacy in Europe*.

electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed."

The PSD2 refers to 'breach' only once, with reference to strong customer authentication (Art. 4 (30)); Art. 96 (1) on breaches refers to operational and security incidents. The NIS Directive features the expression 'breach' three times: twice, in relation to personal data (Recital 63 and Art. 15 (4)), and once, in relation to security. The rest of the text refers to 'incident', as "any event having an actual adverse effect on the security of network and information systems" (Art. 4 (7)).

Three notions can be singled out from this brief survey of definitions: 'breach of security', 'loss of integrity', and '(security) incident'. I argue that these notions converge, with the partial exception of 'loss of integrity'. To prove my point, it is necessary to make a digression on network and information systems, and the equivalence between information and data. Let us start with the term (security) incidents. As seen, the NIS Directive defines 'incident' as an event negatively affecting the security of network and information systems. Network and information security is defined as "the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems" (Art. 4 (2)).

Availability, authenticity, integrity and confidentiality are classic information security goals or canons,[34] or criteria used to assess the good level of security of network and information systems (as is authentication, referred to in Art. 4(30) of the PSD2).[35] Integrity is the opposite of "the accidental or unlawful destruction, loss, alteration" and confidentiality is the opposite of "unauthorised disclosure of, or access", contained in the definition of 'data breaches' provided by the e-Privacy Directive. According to the NIS Directive, information systems are either a (group of interconnected) device(s) which perform automatic processing of data pursuant to a program (Art. 4 (1)(b)), or digital data processed by information systems and networks "for the purposes of their operation, use, protection and maintenance" (Art. 4(1)(c)). This definition highlights the interrelatedness between data, information systems, and networks. The latter are understood as an electronic communications network within the meaning of Art. 2(a) of Framework Directive. Briefly, an 'electronic communications network' is a transmission system, which permits the conveyance of signals, "irrespective of the type of information conveyed" (note that 'signals' are not defined in the law).[36]

Based on this discussion, I can draw a first conclusion: given the near equivalence of networks in the NIS and Framework Directive,[37] security incidents affecting networks should be similarly construed under both Directives. The same could be said for the PSD2, in that, based on the guidelines developed by the European Banking Agency (hereafter EBA) pursuant to Art. 96 (3) (a), an operational or security incident is one "which has or will probably have an adverse impact on the

[34] International Telecommunication Union, *Security in Telecommunications and Information Technology. An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications* (ITU, Geneva, 2015); European Network and Information Security Agency (ENISA), 'Glossary' (*ENISA*) <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary> accessed 2 February 2015.

[35] Understood as "the property of a source being what it claims to be." European Banking Agency, *Final Report on Guidelines on Major Incident Reporting under Directive (EU) 2015/2366 (PSD2). 15EBA/GL/2017/10* (2017), p. 18.

[36] Commission Implementing Regulation 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact. OJ L 26/48.

[37] Keeping aside the difference between the fact that the NIS Directive only refers to private networks.

integrity, availability, confidentiality, authenticity and/or continuity of payment-related services".[38] Moreover, given the understanding, in the NIS Directive, of information systems as (systems of) data, and network and information security as the preservation of, among others, integrity and confidentiality, I can draw a second conclusion. Accordingly, there is a convergence between 'security incidents' and 'breaches of security',[39] irrespective of the fact that personal or non-personal data are affected, and irrespective of the service exposed to the breach. This conclusion is supported by the legislation itself, and the way in which it has been interpreted. For the legislation, suffice to take as an example Recital 63 of the NIS Directive, whereby "personal data are in many cases compromised as a result of incidents."[40] As for the interpretation of legislation,[41] according to a survey run by the European Network and Information Security Agency (hereafter ENISA) with regard to the Framework Directive,[42] the majority of respondents (54%) said that article 13a covers security of electronic communications together with Article 4 in the e-Privacy Directive (compared to 23% of those who thought Article 13a to be sufficient). This understanding finds its confirmation in technical circles: the Annex to the ISO/IEC Standard 29100 promotes the correspondence between privacy breaches and information security incidents.[43]

Based on the above, I can define cyber security breaches as "an event leading to the [accidental or] unlawful destruction, loss, alteration, unauthorised disclosure of, or access to [personal] data transmitted, stored or otherwise processed in connection with the provision of a given service offered by, or accessible via, network and information systems [or that compromises the availability, authenticity and authentication thereof]." The elements in square brackets are those that are not found across all definitions.

Let us now look into 'loss of integrity'. In most national laws transposing the Framework Directive,[44] the expression was understood to mean loss of continuity, i.e. fruition of a service, due to causes other than the violation of information security canons. Hence, this interpretation is not compatible with the understanding of breach or incident I propose above. However, this understanding is not retained in the revised Art. 13a of the proposed EECC (Art. 40 in the current version), which has been rephrased to address "a breach of security that has had a significant impact on the operation of networks or services" (where significance is defined by the same parameters introduced in the NIS Directive, see Section 3.2.2). However, a loss of continuity due to causes other than the violation of security canons affects availability of data and systems and integrity of data and addressing it contributes to the higher goal of Network and Information Security. In fact, Art. 2 (b) of Commission Regulation 2018/151 clarifies that physical security should be part of an "all-hazard risk-based approach".[45] In the PSD2, 'operational' incidents are not clearly distinguished from 'security'

[38] European Banking Agency (2017), *Guidelines on Major Incident Reporting under SPD2*, p. 18. This is also further corroborated by recitals 7 and 95 of the PSD2, which express elements of NIS as part of the EU cybersecurity policy.

[39] This is further supported by the use of both expressions in the Framework and NIS Directive.

[40] See also recital 46 of the NIS Directive, whereby "The security of network and information systems comprises the security of stored, transmitted and processed data".

[41] Furthermore, the Court of Justice of the European Union decided that the confidentiality of communications is part of the essence of the right to respect for private and family life, whereas "the security, confidentiality and integrity of that data" is part of the essence of the right to the protection of personal data. Respectively Judgment of 8 April 2014 in Digital Rights Ireland and Seitlinger and Others, Joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, § 39; Opinion 1/15 of the Court (Grand Chamber), ECLI:EU:C:2017:592, § 150.

[42] Dan Tofan, Konstantinos Moulinos and Christoffer Karsberg, *Impact evaluation on the implementation of Article 13a incident reporting scheme within EU* (European Network and Information Security Agency (ENISA), 2015) p. 13.

[43] International Organization for Standarization (ISO), *International Standard ISO/IEC 29100:2011(E) Information technology — Security techniques — Privacy framework* (2011).

[44] European Network and Information Security Agency (ENISA), *Annual Incident Reports 2016. Analysis of Article 13a annual incident reports in the telecom sector* (2017).

[45] Commission Implementing Regulation 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of

incidents. Yet, Annex 1 of the EBA guidelines contains an interesting definition of operational incidents as "stemming from inadequate or failed processes, people and systems or events of force majeure that affect the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services". Moreover, security incidents may stem from "inadequate physical security".[46] These interpretations suggest that the notion of loss of continuity due to environmental elements (such as natural calamities, cables accidentally broken and human error) can be subsumed under the pursuit of NIS, which has a bearing on the goals that the instruments are trying to pursue, as I address in the next section.

3.2. GOAL OF THE REGULATORY FRAMEWORK

Based on the above, it becomes possible to conclude that the legal framework converges on the understanding of breach of security, and the overarching goal of addressing breaches as part of NIS, which, in turn, is a component of cybersecurity. This concerns the violation of security canons affecting information systems and networks (or engendering cybercrimes), in terms of the availability thereof, or the authenticity, integrity and confidentiality of (personal) information, or both. I corroborate this view in the first sub-section. Instruments diverge with respect to sector-specific threats to NIS, of which environmental elements can be part, and the harms that may ensue, which I discuss in the second sub-section. Fig. 1 exemplifies the hierarchy of goals and harms that the legal framework on cyber security breaches tries to address.

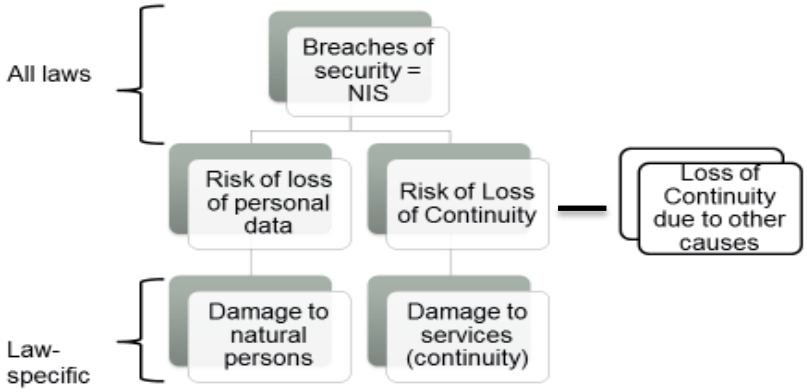

Figure 1 Diagram on harms addressed by legislation on cyber security breaches

3.2.1 The overarching cyber security goal of legislation pursuing breaches

The finding that NIS is the primary concern of legislation addressing breaches is corroborated by an analysis of the articles in which rules on the notification and mitigation of cyber security y breaches are found. In all instruments reviewed here, rules on breaches are placed after provisions laying down an obligation to maintain the security of the service, namely: Art. 19(1) eIDAS Regulation; Art. 14(1) and 16(1) of the NIS Directive, the latter interpreted by Commission

the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact. OJ L 26/48.

[46] European Banking Agency (2017), *Guidelines on Major Incident Reporting under SPD2*, p. 41.

Regulation 2018/151;[47] Art. 32(1) of the GDPR; Arts. 13(a)(1) and (2) of the Framework Directive; Arts. 1 and 1(a) of the e-Privacy Directive; and Art. 95 (1) of the PSD2. All those provisions express a risk-based approach, i.e. they require implementing technical and organisational measures to ensure a level of security appropriate to the risk.[48] Furthermore, provisions on the notification of breaches are also preceded by rules aimed at preventing and mitigating breaches, namely Art. 19(1) of the eIDAS Regulation, Art. 14 (2) of the NIS Directive, Art. 32(1)(c) of the GDPR, Art. 13(a)(1) of the Framework Directive, and to some extent Art. 4(2) of the e-Privacy Directive.

The structure of the articles under analysis, and the overarching goal they express, suggests that notifying a breach to a supervisory authority serves the ultimate goal of addressing harms to NIS, and hence cyber security. This can also be evinced from the European Commission's impact assessment of the GDPR referred to in the introduction, according to which the notification of data breaches serves the highest purposes of 'mutual learning (on the effectiveness of security measures)', 'public awareness' and 'self-improvement' in the area of information security. Some of the instruments explicitly refer to these goals in their recitals, as illustrated in Table 1. Each column refers to one of the six instruments, whereas each row refers to one of the goals of notification.

	e-Privacy	*Framework*	*eIDAS*	*NIS*	*GDPR*	*PSD2*
Mutual learning				Recitals 33 and 34		
Public awareness	Recital 20		Recital 38	Recital 40 and 49	Recital 87	Recital 91
Self-improvement	Recital 20			Recital 4	Recital 87	Recital 91

Table 1 Recitals of legislation and the three goals of notification

3.2.2 Secondary (risks of) damage of cyber security

As discussed above, legislation on breaches aims at either avoiding or reducing the risk of damage to NIS. In turn, maintaining NIS helps avoiding 'secondary' harms that are expressed in the form of risks. Burdon et al.[49] noted that, while the e-Privacy Directive does not qualify the risks 'for personal data and privacy' (Recital 6), Recital 61 of the Citizens' Directive lists the risks that could ensue where a data breach is not addressed in an appropriate and timely manner. Those risks have been transposed into the GDPR. Recital 85[50] refers to "physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned." Moreover, the GDPR distinguishes between different at least five types of risk to the rights and freedoms of natural persons that may lead to damage (Recital 75). The first are generic risks. The second are low risks, as

[47] Art. (2) of the Regulation provides very useful guidance for the understanding of the security requirements. Even though this provision addresses digital service providers (as defined in Section 1.2 and further discussed in Section 5), it could be used, by analogy, in relation to other services.

[48] Article 29 Data Protection Working Party, *Statement on the Role of a Risk-based Approach in Data Protection Legal Frameworks* (14/EN WP 218, 2014); European Network and Information Security Agency (ENISA), *Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools* (2006); Raphaël Gellert, 'Data Protection: a risk regulation? Between the risk management of everything and the precautionary alternative' 5 International Data Privacy Law 3-19.

[49] Burdon, Lane and von Nessen (2012), 'Data breach notification law in the EU and Australia - Where to now?'.

[50] However, consider that recital 61 of the Citizens' Directive and Recital 85 of the GDPR differ.

in the case of pseudonymised data (Art. 4(5) of the GDPR). The third are significant risks, as in the case of special categories of data, a.k.a. sensitive data (Recital 51). The fourth are high risks, which are those that follow a specific assessment, e.g. in relation to data breaches or new technologies.[51] The last, but certainly not least, are data security risks (Recital 83).

Specific risks mentioned in the eIDAS Regulation are financial risks for the trust providers (Recital 37), the risk of loss, theft, damage or any unauthorised alterations to data transmitted via an electronic registered delivery service (Art. 3(36)); risk of misuse or alteration of identity (Art. 8 (2)(a)).

The PSD2 refers to risks relating to security (arguably in terms of information security canons, Recital 91), including "fraud and illegal use of sensitive and personal data (Art. 5 (1) (j)), e.g. "phishing" (Recital 96) and "unauthorized access to the payment account" (Recital 69). The guidelines issued by the EBA that concern the criteria establishing whether a breach should be notified can also be seen as risks. These are: transactions affected; payment service users affected; service downtime; economic impact; level of internal escalation; payment service providers or relevant infrastructures potentially affected; and reputational impact.[52]

The NIS Directive describes risks as "any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems" (Art. 4(9)). Methodologies to quantify harm are scant. If one discounts references to risk in the banking and financial sectors, the rules that concern the criteria establishing whether a breach should be notified contained in Arts. 6, 14 and 16 (and discussed later) offer a proxy for calculating the damage. The entity of damage depends on: (a) the number of users affected by the incident; (b) the duration of the incident; (c) the geographical spread with regard to the area affected by the incident; (d) the extent of the disruption of the functioning of the service; (e) the extent of the impact on economic and societal activities. These criteria have been copied into the EECC (thus redressing the shortcoming of the Framework Directive).[53]

The risks expounded can be associated with harms/damage to natural persons, and harms/damage to the services and society, as exemplified in Table 2.

RISKS	**NATURAL PERSONS**	**SERVICES (AND BEYOND)**
TYPE OF DAMAGE	*Generic, significant, high, security*	*Security and continuity of services*
MATERIAL DAMAGE	• Fraud • Financial loss • Other significant economic disadvantage	• Number of users affected by incident • Economic impact • Other service providers or relevant infrastructures potentially affected • Extent of impact on economic and societal activities and public safety
PHYSICAL DAMAGE	• Mental health • Physical health • Loss of life	• Extent of disruption of the functioning of the service; • Duration of incident • Geographical spread with regard to

[51] The difference between 'significant' and 'high' risks is not immediately apparent; based on an analysis of the relevant provisions, significance seems to concern the intensity of the damage that individuals may suffer from, whereas 'high' seems to concern the likelihood of the damage. An in-depth analysis of the notion of risk in the GDPR is beyond the scope of this paper. However, see the work of Raphaël Gellert, mentioned *supra*, fn. 47.

[52] European Banking Agency (2017), *Guidelines on Major Incident Reporting under SPD2*, pp. 20-21.

[53] Art. 3 of Commission Regulation 2018/151 lays down parameters to determine whether the impact is substantial. In relation to paragraph (a), it indicates the number of contracted natural or legal persons, or the number of affected users based on traffic data.

		the area affected by the incident
NON-MATERIAL DAMAGE	• Alteration, theft or misuse of identity • Damage to reputation • humiliation • other significant social disadvantage	• Reputational impact • Extent of impact on economic and societal activities and public safety
RIGHTS	• Loss of control over personal data • Limitation of rights • Discrimination • Unauthorised reversal of pseudonymisation • Loss of confidentiality of personal data protected by professional secrecy	• Other service providers or relevant infrastructures potentially affected • Extent of impact on economic and societal activities and public safety

Table 2 Summary of instrument-specific harms of cyber security breaches

These may seem to pave the way for multiple combinations of security, continuity and impact on natural and legal persons, as well as society. None of the instruments suggests directly how risks, and related damages, are to be calculated. In some cases, further rules supplement primary legislation; this is the case of implementing acts, e.g. Regulation 2018/151 concerning Art. 16 of the NIS Directive, and of binding guidelines, e.g. those specifying art. 96 of the PSD2.[54] In the Telecom sector, bodies such as the ENISA,[55] and the Article 29 Working Party[56] have provided non-binding examples of risks in relation to breaches. However, no cross-sectorial initiative exists.[57] The private sector has filled in the gap, be it in the form of privately financed studies, such as the one run by the Ponemon Institute,[58] or cyber-insurance[59] that, according to ENISA, has thus far limited adoption compared to other sectors, but may quickly develop with the entry into force of the GDPR and NIS Directives.[60] As a result, even though the instruments[61] and regulatory authorities[62] acknowledge the overlap between the risks to personal and non-personal data, and the fact that breaches can be triggered by cybercrime, there does not seem to be any methodology to survey the combined effect of cyber security breaches across the different sectors.

3.3. MECHANISMS TO MANAGE CYBER SECURITY BREACHES

In order to counter the harms, threats and risks, legislation relies on three approaches: first, the adoption of appropriate technical and organizational measures to counter the breach; second, notification of breaches that are likely to harm; and third, additional tools. Since I discussed the adoption of appropriate technical and organizational measures in Section 3.2.1, therefore here I focus on the remaining two approaches.

[54] European Banking Agency (2017), *Guidelines on Major Incident Reporting under SPD2*.

[55] European Network and Information Security Agency (ENISA), *Technical Guideline on Security measures for Article 4 and Article 13a* (2014).

[56] Article 29 Data Protection Working Party, *Working Document 01/2011 on the Current EU Personal Data Breach Framework and Recommendations for Future Policy Developments (WP 184)* (2011).

[57] Attempts are being made at a higher level of abstraction, which, however, does not embrace privacy rights. A methodology to measure cyber harm was proposed in Agrafiotis and others (2016), *Cyber Harm: Concepts, Taxonomy and Measurement*.

[58] The report covers direct and indirect costs of a personal data breach, both during the crisis and to mitigate the damages suffered by individuals. Ponemon (2017), *2017 Cost of Data Breach Study. Global Overview*.

[59] See, for instance, the policy offered by Zurich: https://www.zurich.com/en/products-and-services/protect-your-business/what-we-protect/cyber-risk (last accessed 19th December 2017).

[60] European Network and Information Security Agency (ENISA), *Cyber Insurance: Recent Advances, Good Practices and Challenges* (2016).

[61] E.g. Recital 63 of the NIS Directive.

[62] Tofan, Moulinos and Karsberg (2015).

3.3.1 Notification

All breached parties must notify the breach to the national regulatory/supervisory authority competent for each instrument. However, notification is 'conditional', in that only breaches that are likely to cause harm to individuals or to services, as discussed in Section 3.2.2, must be notified. This results from, and further feeds into, the incoherence of the concept of notification described by Burdon et al (Section 1).[63] There is no obligation to notify the regulatory/supervisory authority if the breach is either unlikely to result in an appreciable risk to the rights and freedoms of natural persons (Article 33 GDPR),[64] for instance because of the adoption of *ad hoc* or *post hoc* measures of protection,[65] or if the provision of a service is not significantly, substantially, or majorly impacted (Articles 13a(3) of the Framework Directive, 19 (2) of the eIDAS Regulation, 96 (1) of the PSD2, and 14 (3) and 16 (11) of the NIS Directive). Hence, 'significance' (i.e. significant, substantial, major) and 'risk' are the discriminating criteria in notification.

Unfortunately, however, as noted earlier the six instruments do not always provide metrics to evaluate the level of harm.[66] The Framework Directive does not clarify what constitutes a 'significant' impact; ENISA has elaborated some criteria[67] to assess the significance, which are however not mandatory. Moreover, "depending on the national implementation of Art. 13a, if one incident does not affect the continuity of the service (availability), although confidentiality or integrity might be affected, the incident does not need to be reported."[68]

In the NIS Directive, the significance of a disruptive effect depends on the factors listed in Art. 6 (1) and the nature of the essential service, as exemplified by Recital 28. For the health sector, for instance, significance depends on "the number of patients under the provider's care per year. As for water production, significance depends on processing and supply, the volume and number and types of users supplied, including, for example, hospitals, public service organisations, or individuals, and the existence of alternative sources of water to cover the same geographical area". The newly established Cooperation Group is to issue guidelines on the notification of incidents by operators of essential services (Art. 14 (7)).[69] Pursuant to Commission Regulation 2018/151 (Art. 4), an incident is substantial when: the service was unavailable for five million user-hours; 100 000 users suffered from loss of integrity, authenticity or confidentiality of data processed by the digital service provider; the incident put at risk public safety, public security or the life of individuals; and at least one user has suffered from material damage in excess of one million Euros. The Regulation, however, is silent about the case of an incident to a digital service used in the context of essential services, which I discuss later in Section 5.

[63] Burdon, Lane and von Nessen (2012), 'Data breach notification law in the EU and Australia - Where to now?'.

[64] The exception is represented by the e-Privacy Directive, where Telcos must always notify a breach relating to an individual or a subscriber; this exception is however bound to disappear with the overhaul of the e-Privacy Directive.

[65] Commission Regulation 611/2013/EU of 24 June 2013 on the Measures Applicable to the Notification of Personal Data Breaches under Directive 2002/58/EC of the European Parliament and of the Council on Privacy and Electronic Communications (Commission Regulation on Data Breaches); Burdon, Lane and von Nessen (2012), 'Data breach notification law in the EU and Australia - Where to now?'.

[66] The situation may be further complicated by differences resulting from the national transposition of the instruments.

[67] Tofan, Moulinos and Karsberg (2015).

[68] European Network and Information Security Agency (ENISA) (2017), *Annual Incident Reports 2016. Analysis of Article 13a annual incident reports in the telecom sector*, p. 10.

[69] European Commission, *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. Annex to (Communication) COM(2017) 476 final/2* (2017), pp. 26-30.

The proposed EECC lists five mandatory criteria that have been derived from the NIS Directive, but even there, official guidance is needed to enforce a consistent notion of 'significance'. Similarly, to the above, the eIDAS Regulation does not define the key terms 'significant' or 'reliable' used in the notification clauses.[70]

In the case of data breaches, criteria to assess the impact on the rights to data protection and private life ('privacy rights' for short) were developed by the Article 29 Working Party;[71] however, there is no evidence as to the extent to which they were implemented. Under the GDPR, it is the National Data Protection Authority that assesses the likelihood of adverse consequences for data subjects, and can thus still request data controllers to communicate the data breach to affected individuals irrespective of the conditions illustrated above (Art. 34 (4)).

The PSD2 represents an understandable exception, given the longer experience of the banking sector in elaborating cost-benefit analyses and the fact that financial loss is, possibly, easier to quantify. In fact, the EBA's guidelines provide a more nuanced understanding of the notion of 'incident' than other instruments; this is based on a combination of seven criteria which are quantified in absolute and relative terms, and distinguished between lower and higher impact.[72] A major incident depends on the presence of either at least one criterion on the higher-level side of the impact spectrum,[73] or at least three criteria on the lower level side of the impact spectrum.[74] Notification by the payment service provider, which is also due when a low-key incident becomes major as defined above, can be delegated to third parties by means of contracts. Once notified, the competent (supervisory) authority is to further assess the significance of the incident so as to notify relevant national authorities (Art. 96 (1) second indent), as well as the EBA and the European Central Bank (Art. 96 (2)).

Some instruments require notifying supervisory authorities other than the ones responsible for a given sector, such as data protection authorities, or law enforcement authorities (Articles 13a(3) of the Framework Directive and 19(2) of the eIDAS Regulation). When a breach is likely to include two or more Member States, notification should also be made to the responsible authority of the other Member State and the ENISA (Articles 13a(3) of the Framework Directive and 19(2) of the eIDAS Regulation). Pursuant to Art. 96 (2) of the PSD2, the notified competent (supervisory) authority shall notify national authorities that may be affected, the EBA and the European Central Bank, which in turn will assess whether the incident affects more than one Member country (and notifies accordingly).

Moreover, breached parties must notify natural persons, usually when the rights of natural persons are likely to be *adversely affected* by the breach (Articles 4 of the e-Privacy Directive and 19 (2) of the eIDAS Regulation), or there is a high risk thereof (Art. 34(1) GDPR); if the service provider satisfactorily demonstrates that he or she had applied technological protection measures to the

[70] For the standard form, see Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification pursuant to Article 9(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (notified under document C(2015) 7369).

[71] Article 29 Data Protection Working Party (2011), *Working Document 01/2011 on the Current EU Personal Data Breach Framework and Recommendations for Future Policy Developments (WP 184)*.

[72] See in particular table at p. 23 and Annex 1 in European Banking Agency (2017), *Guidelines on Major Incident Reporting under SPD2*.

[73] These are: the affected transactions (more than 25% of the regular level of transactions or five million EUR); the affected payment service users (more than fifty thousand or 25% of the service users), the economic impact (more than Max. or more than five million EUR); and level of internal escalation whereby a crisis mode is likely to be called upon.

[74] These are: the affected transactions (more than 10% of the regular level of transactions, or one hundred thousand EUR); more than five thousand and 10% of users of the payment service; a service downtime of more than 2 hours; a high level of internal escalation; the possibility of affecting other service providers and their infrastructure; and reputational impact.

breached data, then he or she does not have to notify the breach.[75] Under the eIDAS Regulation, legal persons must also be notified. Payment service users must be notified if the incident has or may have an impact on their financial interests (Art. 96 (1) of the PSD2).

Finally, most instruments foresee that, if the authority believes that disclosure of the breach is in the public interest, it may either inform the public, or require the breached party to do so (Articles 13a(3) of the Framework Directive, 19(2) of the eIDAS Regulation and 16(7) of the NIS Directive). Disclosure to the public may also be seen as an alternative for disclosing the breach to individuals, when doing so is either disproportionate, or if otherwise the risk of damage is very low due to the adoption of either *ex ante* measures such as encryption, or of *ex post* measures of mitigation (Art. 34 (3) GDPR). Notification to the public "about individual incidents" may also occur "where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident" under the NIS Directive.

Instruments also differ as to the time that can incur between discovering the breach and reporting it. The most stringent requirement is contained in the guidelines issued by the EBA on the PSD2, whereby payment services providers must initially notify the incident to the competent authority four hours after it was first detected, and provide two additional follow-up on reports.[76] These requirements are followed by the eIDAS Regulation, according to which data breaches must be notified within 24 hours, and by the GDPR (72 hours), whereas the e-Privacy and NIS Directives use the blander expression 'without undue delay'.

3.3.2 Inventories, liability and sanctions

The last of three mechanisms put in place by the six instruments to counter harms of breaches are inventories, liability and sanctions.

Several instruments require keeping inventories of the notification of breaches received. The requirements, however, vary from instrument to instrument. Sometimes the inventory must simply be kept by the services for the sake of the supervisory authority's record (Art. 4(4) of the e-Privacy Directive). In other cases, the national authority must send each year a 'summary report' on the notifications received, either to the Commission (Articles 13(a)(3)) Framework Directive and 17(6) of the eIDAS Regulation) and ENISA, or to the Cooperation Group in anonymised form (Art. 10(3) of the NIS Directive), and explain the actions taken to mitigate the breaches (Framework Directive). As for the GDPR, pursuant to Article 33(5), the controller must document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken, so that the supervisory authority can verify compliance.

The six instruments differ sharply on the question of liability, with the exception, perhaps, of the fact that mostly the laws relate to services, which enjoy a different liability regime than that applicable to goods.[77] Explicit rules are contained in the GDPR, the eIDAS Regulation and the PSD2.

In the GDPR, there are two provisions relevant to liability. The first is the principle of the accountability of the controller, i.e. the party who decides the purposes and means of the processing of personal data, alone or jointly with another controller (Art. 4(7)). Accountability means that a controller is responsible for, and able to demonstrate compliance with the principles relating to the processing of personal data contained in Art. 5 (Art. 5(2)). The effect of this principle is taking a first

[75] E.g. as defined in Commission Regulation 611/2013/EU on Data Breaches.

[76] European Banking Agency (2017), *Guidelines on Major Incident Reporting under SPD2*, pp. 24-27.

[77] On this point, see European Commission, *Building a European Data Economy* ((Communication) COM(2017) 9 final, 2017). The Commission is due to publish an appraisal of the Directive on liability for defective products in mid-2018 European Commission, *Mid-Term Review on the implementation of the Digital Single Market Strategy. A Connected Digital Single Market for All* ((Communication) COM(2017) 228 final, (Staff Working Document) SWD(2017) 155 final, 2017), p.11.

step towards the inversion of the burden of proof. The controller(s) are exempt from liability under the GDPR only if they prove that they are not in any way responsible for the event giving rise to the damage. Otherwise, the second set of provisions, contained in Art. 82 (to be read in the light of Recital 146), apply, namely "any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation." As for processor(s), i.e. the material executor of the processing on behalf of the controller (Art. 4(8)), they are "liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller" (Art. 82). This suggests that liability may apply with or without intention, i.e. also for negligence.

Article 13 of the eIDAS Regulation lays down clear rules for trust service providers. Trust service providers are liable for damages arising from the use of their services, provided this was within the contractual limitations (Recital 37), caused by either intention or negligence, but the burden of proof lies with the natural or legal person claiming the damage. Recital 67 clarifies that website authentication services shall be bound by minimal security and liability obligations. The intention or negligence of qualified trust service providers is presumed, and the burden of proof is inverted. Hence, to address the risk of liability for damage, qualified service providers must either maintain adequate financial resources, or take out appropriate liability insurance, or both. Recital 37 clarifies that these rules should be given effect in accordance with national rules on liability. As for e-identification, Art. 11 lays down that the notifying Member State, the party issuing the electronic identification means and the party operating the authentication procedure, should be liable for failure to comply with the relevant obligations under the Regulation, in accordance with national rules on liability (including the burden of proof, Recital 18).

The PSD2 establishes the principle that each payment service provider is liable for the portion of a transaction that it enables (Art. 92 and Recital 87). Articles 72—74 address the case of unauthorized payment transactions. Pursuant to Art. 73, the payment service provider must refund in full the payer who has suffered from, and has correctly notified, an unauthorized payment transaction (with the possible exception of an excess of 50 EUR); further compensation may be due on the basis of contractual arrangements between the provider and the payer. In such a case, and when the payer claims that a payment transaction was not correctly executed, "it is for the payment service provider [or the payment initiation provider] to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided by the payment service provider" (Art. 72 (1)). The provider is exempted from these rules if it "has reasonable grounds for suspecting fraud and communicates those grounds to the relevant national authority in writing", or if the payer fails to fulfil its obligations under Art. 69 (on personalised security credentials) due to intent or gross negligence. However, pursuant to Art. 72 (2), it is for the payment service provider (or the payment initiation service provider) to "provide supporting evidence to prove fraud or gross negligence on part of the payment service user". This, similarly to the GDPR, provides a step in the direction of a reversed burden of proof. Furthermore, some categories of payment service providers (payment information services and account information services under Art. 5, and payment institutions under Art. 10) are expected to take up professional indemnity insurance to fulfil the safeguarding requirements.

The e-Privacy Directive refers to the liability contained in the Data Protection Directive, whereas the Framework Directive does not address the matter. The NIS Directive contains an explicit reference to the fact that there should be no increased liability attached to the notification of breaches of security – in fact, the reporting done by the single point of contact to the Cooperation Group is supposed to be anonymous. Interestingly, Recital 50 clarifies that "hardware and software products are already subject to existing rules on product liability".

On the matter of sanctions, the GDPR is the only instrument foreseeing a homogeneous system of administrative fines, proportional to the degree of intention, negligence, and gravity of the omission, which can amount to up to 20.000.000 € or 4% of the total worldwide annual turnover of the fined party (Art. 83). The GDPR leaves to Member States the establishment of other penalties for

infringements, which are not subject to administrative fines (Art. 84). The e-Privacy Directive refers to sanctions contained in the Data Protection Directive, which is implemented at the national level and allows imposing pecuniary fines and sanctions of various types. All other instruments refer to the need for identifying effective and dissuasive penalties (art. 16 of the eIDAS Regulation, art. 21 of the NIS Regulation, and Art. 21 of the Framework Directive), but leave the matter in the hand of the Member States, or contracts (PSD2).

4. Assessing the regulatory framework on cyber security breaches

The goal of part 3 was to compare and contrast the instruments that make up the regulatory patchwork of cyber security breaches. Here I set to answer the research question. The sole instruments that can be properly appraised individually, because sufficient time has elapsed, and data have been collected, are those adopted in the first regulatory wave, i.e. the Framework and e-Privacy Directives. Based on the lessons learnt, I subsequently propose a benchmark to evaluate the regulatory framework at the higher level of abstraction (Section 4.2). Subsequently, I illustrate how each individual instrument, as well as the whole framework, fares in relation to the benchmark (Section 4.3). I then discuss the implications of my findings (Section 4.4).

4.1 LESSONS LEARNT FROM THE FIRST REGULATORY WAVE

4.1.2 The Framework Directive

The ENISA has published a number of papers assessing the impact of the norms on breaches – both in relation to security incidents, and loss of integrity (availability) – by means of data collected through regulatory authorities.

As for availability, the regulatory authorities report that the Directive has attained 100% with respect to continuity/availability or disruption/outages of electronic communications networks and services.[78] Interestingly, only 5.1% (34) of the total number of incidents in 2016 was caused by malicious actions (a figure doubled compared to 2015), as opposed to 71% caused by system failures (hardware-related, and software bugs), 12.7 by human error,[79] and 5.1 by natural causes.[80] Denial of service attacks only accounted for 3% of incidents, and network traffic hijack for 1%. As ENISA explains, "The proportion of … cybersecurity related incidents among the total number of incidents reported remains low due to the focus of the [transposition of the][81] recurrent regulation on the "availability" of services and networks, meaning mostly disruptions."[82] In fact, as anticipated in Section 3.1, only a minority of national laws (20%) oblige reporting breaches affecting information confidentiality, or denial of service attacks not necessarily affecting the availability of the electronic communications.[83] ENISA noted that the number of malware-related attacks may be on the rise, in line with the results of statistics worldwide.[84]

[78] Tofan, Moulinos and Karsberg (2015), p. 11.

[79] On the impact of human error, see Wall (2013), 'Enemies within: Redefining the insider threat in organizational security policy'; Ponemon (2017), *2017 Cost of Data Breach Study. Global Overview*.

[80] European Network and Information Security Agency (ENISA) (2017), *Annual Incident Reports 2016. Analysis of Article 13a annual incident reports in the telecom sector*, p. 4 and p. 18. ENISA (2017), p. 4 and then p. 18.

[81] The clarification in square brackets is mine.

[82] European Network and Information Security Agency (ENISA) (2017), *Annual Incident Reports 2016. Analysis of Article 13a annual incident reports in the telecom sector*, p. 29.

[83] Tofan, Moulinos and Karsberg (2015), p. 11.

[84] See, among others, Ponemon (2017), *2017 Cost of Data Breach Study. Global Overview*.

Despite their small reported incidence, malware-related incidents had the greatest impact: they last the longest (90 hours), and consequently entailed the highest number of user hours lost (81500).[85] The cost of insecurity appears therefore high – but how did the transposed Directive fare in terms of security? One fourth of the responding regulatory authorities believe that the requirements contained in Article 13a of the Framework Directive did not lead to stronger security measures; 45% declared not to know what impact the Directive had had on security,[86] a figure that appears disconcerting in itself, and all the more if compared with the 100% on disruption of service mentioned earlier.

The main challenges that regulatory authorities report having faced when they supported providers in the implementation of security measures could offer an explanation as to this result. The biggest challenges were the reluctance of some of the providers in implementing the new regulations (27%), followed by available budget and the administrative burden (25%), and the limited value for money as an outcome of the overall process (21%). ENISA reports that "another challenge in the implementation process of the security measures has to do with the lack of precision in the definition of 'critical assets' and other key concepts such as 'appropriate level of security'".[87] In the same report, ENISA notes that "it is difficult to link the improvement of security measures with the evolution of the number of incidents experienced",[88] but on the bright side, the implementation of Art. 13a has improved the security of smaller or less advanced operators previously needing "technical assistance and know-how".[89]

The difficulty in assessing the success of the Framework Directive in improving the state of network and information security of Telcos has partly to do with the restricted and, arguably incomplete, transposition of the obligations contained in Art. 13(a)(1). However, the indeterminate impact of the Directive is *per se* an important outcome. The current state of implementation of the Directive fails to build on the complementarity (mentioned *supra*) with the e-Privacy Directive highlighted by 54% of national regulatory authorities.[90]

4.1.2. The e-Privacy Directive

Assessing the e-Privacy Directive appears to be even more complex than the Framework Directive. Since supervisory authorities are not required to maintain a record or inventory of the breaches, no comprehensive data is available. Early assessments of the e-Privacy Directive, such as the report conducted for the European Commission by Kosta and Dumortier,[91] do not cover the issue of data breaches.

Annex 8 of the Impact Assessment of the proposed GDPR contains the results of consultations run with SMEs,[92] whereby "most respondents (71.5%) have never experienced a data breach. Among the 7.1% of SMEs that state having experienced breaches, 1.6% related to data being lost, 2.1% stolen and 3.4% misused…Among the SMEs that experienced breaches, roughly half (i.e. 3.9% of SMEs consulted) informed the individuals whose data were affected by breaches, whereas the other half did not. Regarding the cost of the notification to affected individuals, respondents indicated that the notification cost: less than €500 (for 1.6% of SMEs consulted), in the range €501-1000 (for 0.5%), in

[85] European Network and Information Security Agency (ENISA) (2017), *Annual Incident Reports 2016. Analysis of Article 13a annual incident reports in the telecom sector*, p. 28.
[86] Tofan, Moulinos and Karsberg (2015), p. 17.
[87] Ibid, p. 16.
[88] Ibid, p. 17.
[89] Ibid, p. 18.
[90] Ibid, p. 13.
[91] Eleni Kosta and Jos Dumortier (eds), *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation* (Timelex and Spark Legal Network and Consultancy Ltd, 2015).
[92] European Commission (2012), *Commission Staff Working Paper SEC(2012) 72 final*, pp. 131-140.

the range €1001-2000 (for 0.8%) and in the range €2001-5000 for only one single respondent (0.3%)."[93]

In the impact assessment accompanying the proposed e-Privacy Regulation, the Commission reported, based on information collected by Deloitte,[94] that very few Member States have shared information on data breaches,[95] notably the UK and Ireland. According to the assessment performed by Deloitte on behalf of the Commission,[96] the e-Privacy Directive has only been partly effective, efficient, relevant and coherent, though there is room for improvement because the instrument has added value due to the transnational effect of data breaches.[97]

This brief survey does not allow drawing conclusions concerning the ability of the e-Privacy and Framework Directives to avoid harms specific to individuals and services in the Telecom Sector, let alone avoid harms to NIS. Such outcome calls for the need of a specific methodology.

4.2. A BENCHMARK FOR APPRAISING THE REGULATORY FRAMEWORK

Earlier I introduced the three advantages of breach notification identified by the European Commission.[98] I dubbed these three advantages of notification as 'mutual learning (effectiveness of security measures)', 'public awareness' and 'self-improvement' in the area of network and information security. The fact that these goals were suggested in the context of the GDPR makes them a suitable benchmark to assess the adequacy of the framework in relation to personal data breaches. However, since the three goals of breach notification explicitly refer to the overarching goal of all six instruments, i.e. NIS, therefore I suggest they may be used to assess the performance of the legal framework on cyber security breaches. In order to use these goals as a benchmark, it is necessary to give them substance. To do so, I experimentally rely on legislation, policy documents and literature. Some of the sub-goals are relevant for more than one goal, as illustrated in Table 3 below.

MUTUAL LEARNING	**AWARENESS**	**SELF-IMPROVEMENT**
Inventories based on complete and consistent data collection, including reference to technology		Coherent regime on liability for personal data
Consistent notification, including standard timing		Coherent regime on burden of proof
Threat-sharing exercise	Effective supervision	Incentives for the implementation of security measures, including sanctions and rewards

[93] Ibid, p. 133.

[94] Deloitte, *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector. A study prepared for the European Commission DG Communications Networks, Content & Technology* (2017), pp. 111-123.

[95] European Commission, *Impact Assessment Accompanying the document Proposal for a Regulation on Privacy and Electronic Communications* ((Staff Working Document) SWD(2017) 3 final, 2017), p. 123. Indeed, the Information Commissioner's Office published on its website data concerning a variety of breaches of security per sector from 2015 until the present. One such sectors is 'online technology and telecoms', which was exposed to 59 breaches of security in the period surveyed (April 2015-December 2016). Unfortunately, the sector may have been defined so as to include categories beyond the scope of the e-Privacy Directive.

[96] Deloitte (2017), *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector. A study prepared for the European Commission DG Communications Networks, Content & Technology*, pp. 111-123.

[97] As demonstrated by pan-EU data breaches, discussed in Malatras and others (2017), 'Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities'.

[98] European Commission (2012), *Commission Staff Working Paper SEC(2012) 72 final*, p. 100.

Coherent definition of risks	Mechanisms to make the public aware of security stance

Table 3 Benchmarks for the evaluation of legislation on cyber security breaches

Mutual learning and awareness share two intertwined sub-goals. The first is the availability of inventories of cyber security breaches based on complete and consistent data collection exercises, which includes the technology involved. This should be self-explanatory. It means calling the same phenomena by the same names, and keeping statistics on incidents affecting the security technology deployed, irrespective of the harm caused by the incident, with a view to assess the relative strength of a technological solution *vis-à-vis* other, alternative solutions. Different technologies, in fact, are exposed to different risks, and require specific solutions. Hence, surveying the technology involved in breaches is crucial for the sake of mutual learning of security solutions, and self-improvement of businesses and services. However, this goal finds its roots also in legislation and policy evaluation. Article 14 of the Directive on attacks against information systems[99] requires Member States to put in place a system for the recording, production and provision of statistical data on offences including illegal access and illegal interference, to which breaches relate. Consistency in the data collection enables relating cyber security breaches to the relevant criminal law provisions (what is the equivalence between incidents, breaches, attacks etc.), thus enabling an effective response. Moreover, it finds its roots also in the experience that can be derived from the Telecom Framework, whose early appraisal is very difficult because of the scarcity[100] of data.

The second, partly related sub-goal, concerns consistent notifications across sectors (possibly with coordinated timings), which is crucial for the sake of the data collection referred to above, and has been raised as a desideratum by national data protection authorities in the study of the e-Privacy Directive conducted by Deloitte.[101]

Mutual learning can be further measured by two other goals. The first is engaging in threat-sharing exercises, which is derived from the Ponemon Institute's report on the cost of data breaches, according to which it reduces the individual cost of breached records.[102] This can be done under the aegis of the supervisory authority, and thus supports the sub-goal of effective supervision. The second is a coherent and consistent definition of risks. This is derived from the appraisal by ENISA, and the Working Party 29, of the norms on data breaches in the Telecom Framework.[103]

Awareness can be measured by effective supervision, which entails that a competent and agile body deal with the overall management of breaches, and that there is coordination between supervisory authorities; this is derived from observations of the regulatory framework and the review of the e-Privacy Directive,[104] and is supported, by analogy, by Peters' analysis of the US data breach

[99] Directive 2013/40/EU of the European Parliament and the Council of 12 August 2013 on Attacks against Information Systems and Replacing Council Framework Decision 2005/222/JHA, OJL 218.

[100] Tofan, Moulinos and Karsberg (2015); European Commission, *Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC Accompanying the document Proposal for a Regulation on Privacy and Electronic Communications* ((Commission Staff Working Document) SWD(2017) 5 final, 2017).

[101] Deloitte (2017), *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector. A study prepared for the European Commission DG Communications Networks, Content & Technology*.

[102] Ponemon (2017), *2017 Cost of Data Breach Study. Global Overview*.

[103] European Network and Information Security Agency (ENISA) (2017), *Annual Incident Reports 2016. Analysis of Article 13a annual incident reports in the telecom sector*; Tofan, Moulinos and Karsberg (2015); European Network and Information Security Agency (ENISA) (2014), *Technical Guideline on Security measures for Article 4 and Article 13a*.

[104] Deloitte (2017), *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector. A study prepared for the European Commission DG Communications Networks, Content & Technology*.

regime.[105] Awareness is also measured by the availability of mechanisms to warn the public of the ability of an entity to secure information and services. This is self-explanatory, and can include both the obligation to notify to the public, and individuals. This sub-goal is shared with the last goal, which is fostering the self-improvement of breached entities, as the fear of bad reputation can represent an incentive to prevent breaches from happening.

Self-improvement is specifically measured by three additional sub-goals. The first concerns the coherence of the incentives put in place to enforce security measures. The second is liability, and the third is its corollary of the burden of proof. Actually, liability, burden of proof and sanctions are different sides of the same coin. Their viability is supported by the extensive work on the state of information security,[106] ENISA's review of the Framework Directive,[107] work such as that conducted by the Expert Group on Cloud Computing Contracts[108] and, by analogy, by Peters' analysis of the US data breach regime.[109]

this is relevant for section on organizational measures: clash of instruments

4.3. APPRAISING THE CURRENT REGULATORY FRAMEWORK

The legal analysis conducted in Section 3 allows evaluating the question of notification to authorities, to the public, inventories, liability, burden of proof and sanctions. In each table, rows contain the relevant regulatory instruments, whereas columns illustrate, in turn, notification to authorities and the public (Table 4); maintenance of inventories (Table 5), where the symbol X means 'presence', while an empty cell means that, in the corresponding instrument, the specific requirement is absent; and liability, burden of proof and sanctions (Table 6). In tables 4 and 6, 'N.A.' means that the instrument does not mention the item.

	Notification to national authority	**Notification to individuals concerned**	**Notification to general public**
e-Privacy Directive	Always	If Adverse effect, conditional	N.A.
GDPR	If Risk	If high risk, conditional	As substitute to notification to individuals
Framework Directive	If significant impact	N.A.	If public interest
eIDAS /authentication	If impact on cross-border reliability	N.A.	N.A.
eIDAS/ trust services	If significant impact	If adverse effect (also legal person)	If public interest
PSD2 Directive	If major operational or security	If impact on financial interests	
NIS/ essential services	If significant impact	N.A.	To prevent incident/deal with it
NIS/ digital services	If substantial impact	N.A.	If public interest

Table 4 Comparison of rules on notification

[105] Peters (2015), 'So You've Been Notified, Now What? The Problem with Current Data Breach Notification Laws'.

[106] Among others, see Anderson and Moore (2006), 'The Economics of Information Security'.

[107] Tofan, Moulinos and Karsberg (2015).

[108] Whose papers can be found at http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm.

[109] Peters (2015), 'So You've Been Notified, Now What? The Problem with Current Data Breach Notification Laws'.

	Inventory by businesses	**Summary by authority**	**Summary of actions taken by authority**	**To Commission**	**To ENISA**	**To other body**	**Optional threat sharing**
e-Privacy Directive	X						
Framework Directive		X	X	X	X		
e-IDAS Regulation.		X		X			
PSD2 Directive					X	X	X
NIS Directive		X	X			X	X

Table 5 Comparison on rules on inventories and data sharing

	Liability	**Burden of proof**	**Fines/Sanctions**	**Insurance**
e-Privacy Directive	As in Data Protection Directive	N.A.	As in Data Protection Directive	N.A.
GDPR	For intent and negligence	Tilted on the controller or joint-controller	Up to 20.000.000 € or 4% of global annual turnover	N.A.
Framework Directive	N.A.	N.A.	National law	N.A.
eIDAS /authentication	For intent and negligence of Member State/ issuing party/authenticating party	National law	National law	National law
eIDAS/ trust services	For intent and negligence	On natural/legal person	N.A.	N.A.
eIDAS/ qualified trust services	For intent and negligence	Inverted	National law	Y
PSD2	Services: For intent and negligence. Payers: for intent and gross negligence	Tilted on the payment service provider	Left to contracts	Y (some categories)
NIS Directive	N.A.	N.A.	National law	N.A.

Table 6 Comparison of rules on liability, sanctions, burden of proof and insurance

Overall, each instrument contains provisions fulfilling, at least in part, each of the three goals. However, what the tables clearly show is that there is no consistency between the measures adopted in the different instruments. The risk is that of engendering a cacophony that hinders the overall achievement of the three goals, thus reducing the ability to counter cyber security breaches. In the next section, I elaborate on the implications of such a cacophony of requirements.

this is relevant for section on organizational measures: clash of instruments

4.4. ISSUES WITH THE CURRENT REGULATORY FRAMEWORK, AND ITS BEARING ON CYBER SECURITY BREACHES

How does the legal framework fare in terms of mutual learning and awareness? The answer tilts, at best, toward indeterminacy. The absence of a uniform obligation to collect statistics stands in the way of assessing the exposure to breaches, and putting in place adequate solutions. The case of the e-Privacy Directive is in point. Supervisory authorities are not required to maintain a record or

inventory of the breaches. Hence, there is no comprehensive data, which would need to be collected directly from the data protection authorities of each Member State. As seen above, in its (externally done) evaluation of the e-Privacy Directive, the European Commission reported that few Member States have shared information on data breaches.[110] This makes it very difficult to develop mutual learning on the functioning of the security measures within one framework, let alone across several ones.

Seen in this light, the fact that 45% of the national regulatory authorities declared not to know what the impact of the requirements contained in article 13a of the Framework Directive was on security seems less surprising.[111] Part of the problem has to do with the understanding of 'risks' transposed into national law, as I will discuss shortly. In its 2015 report, ENISA noted that "it is difficult to link the improvement of security measures with the evolution of the number of incidents experienced". [112] This suggests that the legal framework may be failing the first goal.

The revised instruments do not seem to be remedying the need for more complete and accurate data: none of the instruments specifically requires collecting comparable data. As seen, there is no common mandatory labelling to classify the incidents, which is amplified by the variety of terms used to refer to breaches in the legislation (discussed in Section 3.1). An easy solution could be to build on the work done thus far by ENISA in mapping trends of threats and incidents.

Still on the issue of inventories, none of the instruments revised apart from the PSD2 require collecting information about the technology involved in the breach. Part of the question may have to do with the underlying technology neutrality of the instruments revised; while a discussion of the merits and limits is beyond the scope of this research,[113] nevertheless in the case at hand the lack of reference to the technology involved in breaches may be counter-productive. In fact, services covered by different legal instruments rely on the same technology. One case in point is that of cloud computing services, addressed by the NIS Directive, which essential services (such as IXPs), as well as trust services (e.g. e-signatures), rely upon. Many providers of public electronic communications services also rely on cloud, e.g. not least for email services. It is interesting to note that ENISA picked on this point in its 2017 report, whereby "the NIS Directive and the new EECC converge on the incident reporting, as many cloud services of DSPs and digital infrastructure of ESOs share common resources coming from telecom providers."[114] The EBA guidelines on the notification requirements of the PSD2 contain commented templates for the initial, intermediate and final reporting of major incidents.[115] Part B3 of the intermediate report, titled "incident description" is intended to collect information on the technology involved in the incident. This, and other parts of the notification template, could be adopted more widely across the patchwork, possibly after revisions to include all substantive categories of cybercrime recognized in Union law, to enable comparable data collection on breaches across sectors.

The understanding of risks is a problem even within single instruments. As seen in relation to the Framework Directive, ENISA reported that a challenge in the implementation of security measures concerns the imprecise definition of 'critical assets' and 'appropriate level of security'.[116] A common definition of risk, crucial for mutual learning (but also self-improvement), may be in sight. ENISA noted, "The NIS Directive and GDPR will affect the regulatory obligations in the Telecom sector, requiring new procedures and more dimensions of information security compliance. The NIS

[110] European Commission (2017), *SWD(2017) 5 final*.

[111] Tofan, Moulinos and Karsberg (2015), p. 17.

[112] Ibid.

[113] Bert-Jaap Koops, 'Should ICT Regulation be Technology Neutral?' in Bert-Jaap Koops and others (eds), *Starting Points for ICT Regulation* (TMC Asser Press 2005); Chris Reed, 'Taking Sides on Technology Neutrality' (2007) 4 Script-ed.

[114] European Network and Information Security Agency (ENISA) (2017), *Annual Incident Reports 2016. Analysis of Article 13a annual incident reports in the telecom sector*, p. 30.

[115] European Banking Agency (2017), *Guidelines on Major Incident Reporting under SPD2*, Annex 1.

[116] Tofan, Moulinos and Karsberg (2015), p. 16.

Directive will introduce new requirements in the area of security measures and incident notification for Digital Service Providers (DSP) and Essential Services Operators (ESO)."[117]

Reaching a common understanding of risks would require, if not regulatory intervention, at least cooperation between national regulatory authorities. However, this may be hampered by the proliferation of responsible authorities. This is a problem even within single sectors: cooperation is hindered by the lack of single contact points, language and applicable law issues, as well as lack of coordination procedures.[118] These issues are amplified across different instruments. The Telecom package assigned responsibility to two different types of regulatory authorities: Telecoms Ombudspersons, and National Data Protection Authorities. Responsibility for the monitoring of breaches under the eIDAS Regulation and NIS Directive[119] are likely to be assigned to different regulatory/supervisory authorities. Cooperation is, as much as supervision (crucial for awareness), sectorial and piecemeal, and may well lead to failing to grasp the bigger picture. In this respect, the fact that the NIS and eIDAS Regulation impose cooperation between the supervisory authority and the NDPA in case of a data breach, with ENISA in case of incidents involving two or more states, and with law enforcement authorities whenever incidents are triggered by computer-related crime is welcome. Best practice may build upon the recent cyber exercise coordinated by the Joint Research Centre, [120] and those carried out by ENISA to achieve strategic, operational and technical convergence.[121]

The question as to whether the legal framework is achieving the goal of self-improvement is also hard to answer. In its appraisal of Art. 13(1)(a) of the Framework Directive, ENISA noted that almost one third (27%) of regulatory authorities were faced with reluctance from Telcos in implementing the new regulations.[122] The last Eurostat poll[123] on network and information security revealed that 60% of businesses in the field of information and communications have a security policy in place, which, in line with current practice, is the first step for fulfilling the risk management approach required by Art. 13(1)(a) of the Framework Directive. In this context, 60% appears too low a figure; it leads to wonder whether a strong liability framework could have pushed businesses to comply. To be sure, there are opinions that discount the usefulness of tougher regulations and new laws, such as the Cyber Rehab project,[124] which proposes to improve internet hygiene through cooperation and offering incentives to service providers that act as good netizens. However, the project itself suggests 'punishing' the non-compliant internet service providers by excluding them from peering agreements, thus losing their infrastructure. In agreement with Peters, [125] adequate liability and sanctions may be the only way to force companies to adopt adequate security measures to protect information and services.

The questions of liability and of the wider implications of the regulatory framework is best discussed in relation to cloud computing.

---

[117] European Network and Information Security Agency (ENISA) (2017), *Annual Incident Reports 2016. Analysis of Article 13a annual incident reports in the telecom sector*, p. 30.

[118] Malatras and others (2017), 'Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities', p. 459.

[119] The Commission seems to be aware of this with reference to NIS; its discussion of ENISA's work on national approaches to Critical Information Infrastructure Protection, and particularly the case of Sweden, could lead to a blueprint for cooperation which could be useful in the case of breaches of security. European Commission (2017), *Making the most of NIS*, p. 13.

[120] Malatras and others (2017), 'Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities'.

[121] Ibid, p. 463.

[122] Tofan, Moulinos and Karsberg (2015), p. 17.

[123] Eurostat data available at http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises.

[124] John Leyden, 'CyberRehab's mission? To clean up the internet, one ASN block at a time' *The Register* (31 August 2017).

[125] Peters (2015), 'So You've Been Notified, Now What? The Problem with Current Data Breach Notification Laws'.

5. Implications of the regulatory patchwork: the case of cloud computing

Since cloud computing is a technology common to all legal instruments revised in this paper, as well as a technology powering today's use of the Internet and enabling the so-called datafication and the ensuing data economy,[126] it is a case in point to show the drawbacks of the inconsistencies of the patchwork of laws regulating breaches of security. I begin by briefly positioning cloud computing in EU law. I then discuss the rules applicable to cloud computing contained in the NIS Directive. Subsequently, I appraise how the rules contained in the NIS Directive interact with the rules contained in the GDPR. The result reinforces the feeling of indeterminacy paved for by the regulatory patchwork (and leads to question whether this state of affairs maintains the insecurity of services, leading to further breaches).

5.1 CLOUD COMPUTING IN EU LAW

The NIS Directive defines cloud computing as "a service that enables access to a scalable and elastic pool of resources" (Art. 4(19)). Resources refer to both computational power and storage space. Scalability and elasticity are not defined, but the first commonly means that resources can be increased or decreased as needed, while the second refers to the fact that different users employ the service differently within the day.[127]

Public clouds are usually further classified into three categories, namely software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS).[128] The first includes the use of software stored remotely, e.g. email services or document compilation services. The second usually refers to the use of server space for computational power or storage. The third usually refers to services, such as software, that can be tailored by users, or platforms for the production of software applications, or databases.[129]

In the NIS Directive, cloud computing is defined as a digital service, which falls within the broader category of information society services. These are defined in the amended e-Commerce Directive[130] as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services". For the purposes of this definition: "(i) 'at a distance' means that the service is provided without the parties being simultaneously present; (ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request."

[126] European Commission (2017), *(Communication) COM (2017) 9 final*.

[127] For further clarifications, see European Commission (2017), *Making the most of NIS*.

[128] For a technical analysis of the cloud, see Michael Armbrust and others, *Above the Clouds: A Berkeley View of Cloud Computing.* (Technical Report No UCB/EECS-2009-28, 2009).

[129] See discussion in European Commission (2017), *Making the most of NIS*, pp. 32-37.

[130] Directive 2015/1535/EU of the European Parliament and of the Council of 9 September 2015 Laying down a Procedure for the Provision of Information in the Field of Technical Regulations and of Rules on Information Society services (codification), OJ L 241.

5.2 THE CLOUD AND CYBER SECURITY BREACHES

The NIS Directive seeks to "ensure a high level of harmonisation for digital service providers with respect to security and notification requirements … in a manner proportionate to their nature and the degree of risk which they might face". The nature of cloud computing, as seen above, is that of a digital service provider. Unlike operators of essential services, digital services providers do not have a direct link with physical infrastructure, but rather have a "cross-border nature" (Recital 57), and as a result are subject to different notification requirements.

First of all (1), pursuant to Article 16 (10), Member States cannot impose additional "security or notification requirements on" cloud providers than those included in the Directive, and further specified by Commission Regulation 2018/151.[131]

Secondly (2), cloud providers must notify an incident that has a "substantial impact on the provision of a service" (Art. 16 (3)), and for which the provider has "access to the information needed to assess the impact of an incident against the parameters" established by the Directive (Art. 16 (4)). Note that these conditions are formulated in a way that appears cumulative. Moreover, 'substantial' impact is more restrictive than 'significant', which is the criterion used in relation to essential services in Art. 14(3). In fact, in addition to the parameters identified for operators of essential services, the article lists two further criteria (of fthe list in Art. 6), to judge the impact of an incident. These criteria have been clarified by Commission Regulation 2018/151 (Art. 3), and are: "(d) the extent of the disruption of the functioning of the service", understood in terms of information security canons; and "(e) the extent of the impact on economic and societal activities", to be assessed in relation to the nature of the contractual relation with the customer or the number of users affected, or *significant* material or non-material losses, e.g. in relation to health, safety or damage to property. I will come back to this point in Section 5.3.

Thirdly (3), disclosure of the incident suffered by cloud providers to the public is not mandatory but, differently from the case of operators of essential services, dissemination can nonetheless be decided, "where disclosure of the incident is otherwise in the public interest" (Art. 16 (7)). Moreover, these rules do not concern small or micro enterprises[132] (Art. 16 (11)).

Fourthly (4), supervisory measures should take place *ex post facto* (article 17). Recital 60 clarifies that "digital service providers should be subject to light-touch and reactive *ex post* supervisory activities justified by the nature of their services and operations. The competent authority concerned should therefore only take action when provided with evidence … that a digital service provider is not complying with the requirements of this Directive, in particular following the occurrence of an incident".

Finally (5), the regime for sanctions and liability is left to each Member State, according to national law.

Table 7 summarises the findings. Each point discussed in the text is marked by a number, e.g. (1), and is synthetically shown in the box corresponding to the relevant sub-goal of the benchmark. Table 7 shows that, in the case of cloud computing, the Directive fails one or more sub-goals, which are struck-off and substituted by a blander rule.[133]

[131] As discussed earlier, in section 2.2.1. Rather, the Directive seems to imply that additional security requirements may be imposed on public-sector bodies (Recital 56).

[132] Small enterprises are businesses with less than 50 people and a turnover below 10 million €; micro enterprises are businesses with less than 10 people and a turnover of less than 2 million €. According to Eurostat, they represent the majority of EU enterprises: European Commission (2012), *Commission Staff Working Paper SEC(2012) 72 final*, p. 118.

[133] For criticism of the NIS Directive beyond the cloud, see Rebecca Wong, *Data Security Breaches and Privacy in Europe* (Springer 2015), chapter 10.

MUTUAL LEARNING	**AWARENESS**	**SELF-IMPROVEMENT**
Inventories based on complete and consistent data collection, including reference to technology		~~Coherent regime on liability~~ Sanctions and liability left to each MS (5)
~~Consistent notification, including standard timing~~ Notification by cloud provider due only if incident is substantial + "provider has "information to assess impact" (2)		~~Coherent regime on burden of proof~~ Standard burden of proof (5)
Threat-sharing exercise	~~Effective supervision:~~ Supervision is ex post, prompted by evidence (4)	~~Incentives for security measures~~ MS cannot impose strict security requirements (1)
Coherent definition of risks	~~Mechanisms to make the public aware of security stance~~ Public notification is not mandatory (3)	

Table 7 Benchmarks appraised in relation to rules applicable to cloud computing.

Such rules may reflect the reality of a market composed of mostly extra EU service providers. Indeed, the main cloud market players - Amazon, Google, Hewlett Packard, IBM, Microsoft, Joyent cloud, Rackspace, Salesforce.com and VMware (which does not provide hosting services) – are based in the United states. According to the Synergy Research Group, the cloud infrastructure leader for the third quarter of 2016 was Amazon AWS, which alone had more than 40% of the market share.[134]

It is hard to come by figures that indicate the share of these players, as well as the European ones,[135] in the European market. Recent Eurostat data shows that the cloud is used by 21% of EU enterprises, with lows of 20% in essential services and of 54% in ICT. Most enterprises rely on the cloud for email and storage of files, with clear implications for personal data.[136] To increase the adoption of cloud by enterprises in the EU, the European Commission launched the Cloud initiative, which is hoped to strengthen "Europe's position in data-driven innovation, improve competitiveness and cohesion, and help create a Single Digital Market in Europe".[137] A limiting factor identified by the Eurostat survey seems to be the fear of breaches of security. This fear is not ungrounded, as shown by the many reported leaks of Amazon's AW3 buckets,[138] as well as news of a malicious 'search engine' to accesses firms' sensitive documents held in those buckets.[139] Moreover, in its 2017 report, the Ponemon Institute calculated that the cost *per capita* of a breach increases by USD 14.3 in case of extensive cloud migration; this figure reaches USD 16.3 in case of third party involvement (sub-contracting is not unusual in the case of cloud).

The information at hand is insufficient to claim once and for all whether cloud computing undermines rather than support NIS, but rather seems to confirm the point made earlier on the need to collect data on cyber security breaches that duly takes technology into account. However, the fact that provisions on cloud computing contained in the NIS Directive fail in different respects the three sub-goals (starting from the noticeable point that Member States cannot impose higher security requirements on cloud providers than those agreed at EU level) has an immediate impact on securing

[134] See at: http://www.itmanagerdaily.com/cloud-computing-vendors/.

[135] A list of top IaaS European players can be found at: https://www.channele2e.com/channel-partners/csps/top-10-european-cloud-services-providers-csps-for-iaas-list/.

[136] Available at: http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises.

[137] Quoted from <https://ec.europa.eu/digital-single-market/en/%20european-cloud-initiative>. See also European Commission (2017), *(Communication) COM (2017) 9 final*.

[138] Ali Fahad, 'Open AWS S3 Bucket Leaks Hotel Booking Service Data' *AWS News* (22 August 2017). Stylianou et al. note how cloud providers, including IAAS, are not committed to adequate security. Stylianou et al., 2015, 'Protecting user privacy in the Cloud: an analysis of terms of service' 6 European Journal of Law and Technology, p. 10.

[139] I am grateful to Prof. David Wall for pointing me to this. BBC, 'Search tool accesses firms' documents in the cloud' *BBC* (14 February 2018).

the cloud, and may ultimately counteract the positive efforts of the regulatory patchwork, as I discuss next.

5.3 THE PATCHWORK AND THE CLOUD: THE CASE STUDY OF HIGHER EDUCATION INSTITUTIONS INCLUDING TEACHING HOSPITALS

The NIS Directive distinguishes between the case of a cloud provider offering its services to an essential operator and to any other businesses. Here I wish to discuss how the rules would play out in the case of higher education institutions (i.e. universities) featuring a teaching hospital. Higher education institutions, which are a big data producer and repository, rely amply on cloud solutions. As a result, they are exposed to breaches affecting cloud services. As for the UK, the Times unveiled that, in 2016-17, higher education institutions that had responded to its freedom of information requests had suffered from 1100 breaches. These resulted from distributed denial of service (DDoS) attacks, spam, and ransomware, and aimed at intellectual property resulting from years of research, non-sensitive personal information to carry out identity theft and loss of patients records.[140] On top of that, a breach of security of cloud services offered to the teaching hospital branch of the higher education institution could affect the distribution of drugs to patients, the triage system of A&E, and the functioning of other basic hospital services. This case is interesting because it embraces both sets of rules applicable to digital service providers. The teaching hospital is affected by the provisions on cloud, which concern operators of essential services. The higher education institution is affected by the rules on cloud offering its services to businesses other than operators of essential services; unless those businesses are covered by sector-specific rules, the NIS rules act as the *lex specialis*.[141]

I begin with discussing the implications of a breach for the teaching hospital. According to a literal interpretation of Art. 16 (5) of the NIS Directive, if a cloud provider suffers from an incident that affects significantly its operation, it would be for the operator of essential services to notify the incident. Neither the Recitals nor the Commission[142] seems to clarify this point, and the reader is left wondering whether the Directive is incorrectly worded.[143] Consequently, the Directive is currently silent about the obligation of a cloud provider offering services to essential service operators to notify a breach without undue delay. Moreover, as I anticipated in the previous section, essential service operators must notify significant incidents, whereas cloud providers must only notify substantial ones, which could create a severe short-circuit in the law (resulting from the incoherence of notification as discussed earlier). The fact that Art. 3 (5) of Commission Regulation 2018/151 implies that a substantial incident is one having a *significant* impact on economic and societal activities may address such short-circuit, because significance is to be assessed sector by sector. An official interpretation of this point is warranted.

Here we can distinguish between the following cases: a breach that does or does not significantly affect the continuity of the services offered by the hospital, and one that does or does not affect personal data (which paves the way for a matrix of four different circumstances). A breach of security that does not concern personal data and is not significant within the remit of the NIS

[140]Peter Yeung and Rosemary Bennett, 'University secrets are stolen by cybergangs. Scientific Research Targeted by Hackers' *The Times* (5 September 2017). These data seem to confirm previous research showing the cybersecurity struggle of UK research and higher education institutions that involved 50 universities commissioned by the cloud provider VMware, mentioned in Chris Havergal, 'UK universities 'losing cyber security battle'' *Times Higher Education* (16 March 2016).

[141] European Commission (2017), *Making the most of NIS*, p. 37. The PSD2 falls outside the scope of the notification rules contained in the NIS Directive (Art. 1 (7) and Recital 12), ibid, p. 37. The same applies to Telecom operators and assurance and trust services (Art. 1 (3)).

[142] European Commission (2017), *Making the most of NIS*.

[143] Which reads "Where an operator of essential services relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified by that operator" (as opposed to "*to* that operator", or "by that *service provider*").

Directive would not need to be notified; this represents clearly the contradiction inherent in the concept of notification highlighted by Bourdon et al. (discussed in Section 1), and constitutes a missed opportunity for mutual learning and awareness. A significant breach affecting non-personal data (e.g. the loss of anonymised medical data for research purposes) would suffer from the lack of clarity concerning the distinction between substantial and significant incidents. A delayed notification could have serious consequences for the hospital, and NIS. Two recitals capable of applying to public operators may suggest a solution to the *impasse*, which could also be followed, by analogy, by private operators. Recital 54 encourages public administrations using services offered by digital service providers to "require from the providers of such services additional security measures…by means of contractual obligations" (Recital 54). Public-sector bodies could also be required "to ensure specific security requirements when they contract cloud computing services", but these measures "should apply to the public-sector body concerned" (Recital 56). Hence, it is envisaged that the matter will be resolved contractually, as currently is the case. Contracts will address responsibility for notification and the ensuing liability in accordance with national laws, which may differ as to, for instance, damages, intention, negligence, burden of proof or relevant applicable procedural rules. This brings us to the question of self-improvement. In the NIS Directive, notification should not lead to increased liability for the notifying party (Art. 14 (3)). Whenever notified, the competent authority shall preserve the security and commercial interests, as well as the confidentiality of the information provided in the notification of both the operator of essential services and digital service providers (Art. 14 (5) and Art. 16 (6)). Rather, whenever possible the notified bodies must provide "information that could support the effective incident handling". The European Commission Expert Group on Cloud Computing Contracts[144] showed how cloud contractors tried to cap and limit their liability. The Group noted that, given how hard it is to assess technical responsibility in the cloud, it could be difficult to follow standard rules on the burden of proof,[145] a conclusion similarly reached by Peters in relation to case law in the US,[146] and which would potentially leave teaching hospitals exposed (and fail to provide incentives for the cloud to improve).

Particularly in the case of data breaches, cloud providers have been known to try to shield responsibility by presenting themselves as processor in cloud contracts,[147] which brings us to the case of breaches of security affecting personal data, where the GDPR is the *lex specialis.*[148] On the one hand, the contract[149] signed between the cloud provider and the hospital will be relevant to assess the cloud's position as either a processor or a joint-controller, according to established interpretation of data protection law. On the other hand, the exact role of the cloud provider will depend on the nature of the processing activities carried out and the degree of involvement in determining the means and purposes of the processing.[150] Pursuant to Art. 33 of the GDPR, the controller or joint-controller should notify a breach to the supervisory authority without undue delay, and the processor should do the same with respect to the controller (though not all breaches are to be notified, with clear losses for the sub-goal mutual understanding). Liability would attach to both, but with a higher threshold in the case of processors as discussed in Section 3.3.2, because the principle of accountability only applies to controller(s). As a controller, the hospital is accountable: to be exempted from liability for the damage caused by processing, it must be able to prove that it is not in any way responsible for the event giving rise to the damage, and to demonstrate compliance with the principles relating to the

[144] See in particular the Discussion paper on "Liability for non-compliance with data protection obligations", Discussion paper on "Unfair terms in cloud computing contracts", and Discussion paper on "Liability" available at http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm.

[145] Ibid.

[146] Peters (2015), 'So You've Been Notified, Now What? The Problem with Current Data Breach Notification Laws'.

[147] Ibid.

[148] Recital 9 of NIS Directive, Art. 2 and European Commission (2017), *Making the most of NIS*, p. 37, note 40.

[149] Simon Bradshaw, Christopher Millard and Ian Walden, *Contracts for Clouds: A Comparative Analysis of Terms and Conditions for Cloud Computing Services* (2010).

[150] Article 29 Data Protection Working Party, *Opinion 1/2010 on the Concepts of 'Controller' and 'Processor'* (2010).

processing of personal data. This include selecting a processor (a cloud provider) that ensures an adequate level of security (Art. 28 (1)). Whilst the provisions inserted in the contract may help, the higher threshold for the notification of breaches to which cloud providers are usually subject (*vis-à-vis* non-personal data), and the lack of access to relevant technical information by the hospital as noted above, may represent an obstacle to the fulfilment of accountability. Moreover, in the time needed to attribute responsibility, individuals may suffer from a cascade of harms. The strength of these rules, and the achievement of the sub-goal of self-improvement, will depend on the dissuasive role played by sanction, as well as the *ad hoc* enforcement of the Regulation in this area. In fact, the GDPR allows Member States to adopt different rules on the processing of data for medical purposes, including requiring controllers to obtain prior authorization from the supervisory authority for processing operations in relation to public health (Art. 36 (5)), which may redress the issues discussed above.

I now move to discussing the implications of a breach for the remainder of the higher education institution. Here again there are differences between types of incidents. As for incidents that do not affect personal data, the fact that the 'incident' must be substantial for it to be notified hinders the achievement of mutual learning and awareness and leaves higher education institutions exposed to damages. The contractual solution proposed by Recitals 54 and 56 of the NIS Directive is likely to be followed here, too, and the issues of lack of technical knowledge to assess responsibility behind the incident may put higher education institutions in a difficult situation. As for incidents that affect personal data, higher education institutions are likely to enjoy the exceptions contained in data protection legislation for data processing for purposes of historical, scientific and statistical research, which are also listed in the GDPR (Art. 89). The considerations made for hospitals in terms of liability and difficulty of fulfilling the principle of accountability also apply here. Similarly, it is interesting to see how national laws will differ on expectations and exemptions made for higher education institutions (in case of mismanagement of personal data).

In conclusion, the interaction between the patchwork, exemplified here by the GDPR and the NIS Directive, leads to indeterminacy, which may undermine the three benchmarks, irrespective of whether the incident concerns personal or non-personal data. The high threshold for the notification of breaches (aimed at minimizing costs for the notifying parties, as noted by Bourdon et al.) for cloud providers means that many incidents may go undetected, which frustrates the goals of mutual learning and awareness. The contractual solution seems to be addressing the symptom, rather than the cause, and may make it difficult to assess responsibility, thus also affecting self-improvement, in what becomes a vicious circle.

According to De Bruin and Floridi, as well as Prüfer, no further legislation should be adopted to spur the adoption of appropriate security measures. De Bruin and Floridi [151] propose to foster 'transparency' of the cloud provider (the ethical principle of translucency). [152] This may redress the fact, noted by Prüfer, that all cloud computing services suffer from adverse selection or the lemons problem, whereby given the "low willingness-to-pay of buyers, only sellers who actually supply low accountability will populate the market."[153] In this respect, Prüfer[154] proposes resorting to certifying authorities and conflict resolution by arbitration. His model has the appeal of economic pareto-efficiency; however, for the certification authority to be impartial and ensure the respect of the bodies of laws in which it operates, and amenable to courts, it would need to be set up itself by a law.

[151] Boudewijn de Bruin and Luciano Floridi, 'The Ethics of Cloud Computing' 23 Science Engineering Ethics 21-39.

[152] Indeed, toothless transparency has led to the jungle of notices reviewed, among others, by Stylianou et al., 2015, 'Protecting user privacy in the Cloud: an analysis of terms of service' 6 European Journal of Law and Technology.

[153] Jens Prüfer, *How to Govern the Cloud? Characterizing the optimal enforcement institution that supports accountability in cloud computing* (2013) p. 35.

[154] Prüfer (2013), p. 35.

Without well-reasoned and well-enforced laws and adequate incentives, we can expect the data economy to foster increasing and ever bigger breaches, particularly in the light of the requirement to increase the flow of non-personal data[155] (including data which is presently anonymised, but which could possibly become re-identifiable with further advances of computing). Incentives mostly concern personal data as contained the GDPR, incentives that have yet to be tested. In fact, the reflections contained in this section are partly speculative, because the GDPR has just entered into force, many of its provisions require national implementation, and the NIS Directive must be transposed into national law. The state of flux of the second wave of regulation, however, may be blessing in disguise, as it leaves room for corrections and interventions *en route*.

6. Conclusions: patching the patchwork

Cyber security breaches are on the rise, one of the reasons being the well-known lack of incentives to secure services and their underlying technologies such as cloud computing, incentives that the patchwork of laws on breaches may be failing to provide. The current legal framework seems to be offering solutions to the symptoms, rather than the causes. Liability of middle users such as data controllers, who rely on third-party cloud applications, and contractual solutions pushing towards the wider take up of cyber insurance, would provide some redress to distressed natural and legal persons,[156] and this would certainly not be a negative result.[157] However, it may leave the real risks, and responsibilities, unaddressed. In fact, legislation on cyber security breaches, whose overarching goal is to ensure an adequate level of information and network security, may be failing to meet the three goals: (i) providing the necessary level of mutual learning on the functioning of security measures; (ii) raising awareness of both regulatory authorities and the public on how entities fare in protecting data; (iii) and enforcing self-improvement of entities dealing with information and services. The second regulatory wave (eIDAS Regulation, the PSD2, the GDPR and the NIS Directive) benefitted from only partial lessons drawn from the first regulatory wave (Telecom Framework) and, since each instrument was adopted independently, it yielded potentially contradictory results. Policy-makers can still redress these issues in the third regulatory wave, but the EECC has the inherent limit of being sector-specific (vertical).

Part of the problem could be addressed by collecting data on breaches that are mindful of the technological environment, but also by an active attempt to create more harmony among the regulatory patchwork. For instance, responsible authorities could cooperate to create a middle-level of integration, with the aim of pursing national convergence of EU law. This could include an observatory of the national legislation adopted with respect to breaches in the different sectors. Such level of awareness may yield best practice, which could be adopted at an EU-wide level.[158] Cooperation by the authorities responsible for different instruments could lead to a common definition of risks, and the measures best suited to address such risks.

Yet, to patch the current patchwork, and with it information insecurity, measures of 'public ordering' are required to incentivise the adoption of better technical and organisational measures, and provide better remedies, as also encouraged by Peters and Bourdon et al.. First, the results of cooperation among national authorities could inform a piece of EU law mandating the consistent, and technology-sensitive, collection of information on cyber security breaches. Collection could be overseen by ENISA, the NIS Cooperation Group, the Data Protection Board, or by the three together.

---

[155] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union. (Communication) COM(2017) 495 final* (2017).

[156] Peters argued that this could be a measure to secure that harmed individuals could obtain redress Peters (2015), 'So You've Been Notified, Now What? The Problem with Current Data Breach Notification Laws'.

[157] As discussed in ibid.

[158] I would like to thank Dr Nicolo Zingales for the suggestion that national private law may contain some of the solutions.

Secondly, it is hoped that a strong implementation of the GDPR will create some of the hitherto missing incentives to protect information.[159] Thirdly, policy makers should seriously discuss introducing liability for security vendors.[160] For instance, Prüfer's idea of relying on certification as a form of private ordering[161] can be espoused with the system of qualified/unqualified trust service providers created by the eIDAS Regulation.[162] There, qualified trust service providers wishing to offer their services to public bodies need to undergo a process of certification, whereby they adhere by certain standards. The process whereby service providers become qualified has the advantage of 'responsibilising' the provider, by also reversing the burden of proof; this could possibly lead to the further expansion of cyber insurance, but in a way in which the causes of cyber insecurity are addressed together with the symptoms. Eventually such an approach may lead to achieve the three goals of mutual learning on the functioning of security measures, awareness of both regulatory authorities and the public on how entities fare in protecting data, and enforcing self-improvement of entities dealing with information and services (thus neutralizing the conceptual incoherency of notification).

Acknowledgments

Early versions of this paper were presented at the Second Annual Cybercrime Conference, University of Cambridge Cybercrime Centre (July 13th 2017); European Society of Criminology 2017 Conference EurCrime, University of Cardiff (September 13th-16th 2017); TILEC-GovReg Workshop, Tilburg University (October 12th-13th 2017); and the Centre for Criminal Justice Studies Public Seminar "Cybercrimes of the Future", University of Leeds (November 6th 2017). I would like to express my gratitude to the organizers and audiences of those events for their helpful comments, and Prof David S. Wall for the conversations that informed the development of this article. I would like to thank in particular Dr Inge Graef, Emeritus Prof Steve Saxby, Lina Jasmontaite and my anonymous reviewers for their precious suggestions on how to improve the draft, Dr Martyn Egan for the continuous support and encouragement. Research for this paper was funded by the EPSRC research project "Combatting cRiminals In The Cloud" (CRITiCal - EP/M020576/1).

[159] I am indebted to Dr Inge Graef for the formulation of this point.

[160] Beyond what hinted at in European Commission (2017), *(Communication) COM (2017) 9 final*.

[161] Prüfer (2013), p. 35. I am indebted to Dr Jens Prüfer for elaborating this passage.

[162] In this respect it will be important to follow the development of the so-called Cybersecurity Act. European Commission, *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013,*

and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"). (Communication) COM(2017) 495 final (2017).