|NST|TUTO
UN|VERS|TÁR|O
DE L|SBOA

Europeanization processes regarding matters of Cybersecurity: the case of Portugal

Pedro Miguel Alexandre

Master in International Studies

Supervisor:
PhD Inês Marques Ribeiro, Integrated Researcher
Iscte – Instituto Universitário de Lisboa

Supervisor:
PhD Carlos Serrão, Associate Professor
Iscte – Instituto Universitário de Lisboa

November, 2020

SOCIOLOGIA
E POLÍTICAS PÚBLICAS

Europeanization processes regarding matters of Cybersecurity: the case of Portugal

Pedro Miguel Alexandre

Master in International Studies

Supervisor:
PhD Inês Marques Ribeiro, Integrated Researcher
Iscte – Instituto Universitário de Lisboa

Supervisor:
PhD Carlos Serrão, Associate Professor
Iscte – Instituto Universitário de Lisboa

November, 2020

Agradecimentos:

Durante o processo de elaboração deste trabalho de investigação, várias foram as pessoas responsáveis pela sua conclusão. De maneira direta ou indireta, estiveram sempre presentes ao longo do meu caminho e sem elas, não conseguiria irrefutavelmente chegar a esta etapa final. Sendo assim, dedico-lhes este agradecimento bastante especial.

Em primeiro lugar, quero agradecer à minha mãe, não só pela constante motivação, mas por ser a primeira e a última pessoa a depositar em mim a sua confiança – especialmente em momentos mais complicados e desafiantes. Sem ela, como em tantas outras situações, nada disto seria possível. A seguir, agradeço à minha orientadora, a Professora Doutora Inês Marques Ribeiro, e ao meu orientador, o Professor Doutor Carlos Serrão, pela paciência, pela ajuda, pela amabilidade, e pela experiência que me disponibilizaram. Foram muitas as ocasiões em que me senti perdido, mas os dois apoiaram-me em todas as minhas etapas e decisões, certificando-se de que estava bem encaminhado.

Em segundo lugar, quero agradecer ao Eduardo André, a primeira pessoa com quem me cruzei durante o meu percurso laboral, que me mostrou não só como ser um bom profissional, mas como trabalhar em equipa, especialmente quando precisava de sair mais cedo para as aulas ou para estudar. O seu apoio incondicional teve um peso crucial ao longo dos meus estudos.

Em terceiro lugar, quero agradecer a todos os meus amigos e familiares, com um destaque à Ana Sofia Franco, por me ter acompanhado durante estes últimos seis anos, mas mais importante nestes últimos dois: por todos os conselhos, todo o apoio e amizade. Em último, quero agradecer a todos os professores e colegas do mestrado em Estudos Internacionais, por me terem ajudado a chegar ao meu tema e por toda a partilha de conhecimento e ideias.

Resumo

Tendo em conta um presente que abraça mais o tecnológico, a questão da cibersegurança tem-se tornado cada vez mais uma realidade diária e é necessário encará-la como algo essencial para a proteção da nossa presença *online*. Não só a nível de boas práticas de navegação na internet, mas também na implementação de ações prontas para combater novas e desconhecidas ameaças: vários são os países que prestaram atenção a estas mudanças e alteraram as suas políticas de segurança. Pretendemos neste sentido utilizar a Europeização para perceber, na esfera da integração europeia, como é que a União Europeia afeta e influencia os seus Estados-Membros na formulação de medidas relacionadas com a cibersegurança dos seus cidadãos. Seguidamente, é prestada uma atenção especial a Portugal, sendo utilizado como um caso de estudo. Esta escolha advém do facto deste país conter literatura académica ainda por explorar sobre o tema, em comparação com outros de maior dimensão. Sendo assim, o objetivo principal deste trabalho é precisamente proporcionar uma nova visão sobre como a UE tem moldado o processo legislativo de um país pequeno no seu tamanho, mas de qualquer forma importante na sua posição no panorama europeu.

Palavras-chave: Cibersegurança; Europeização; Portugal; União Europeia; Internet

Abstract

In a world that receives technology with open arms, the issue of cybersecurity has increasingly become a daily reality and it is necessary to treat it as something essential for the protection of our online presence. Not only in terms of secure internet browsing practices, but also in the implementation of actions that are ready to tackle new and unknown threats: several countries have paid attention to these changes and modified their security policies. In this sense, we intend to use Europeanization in order to understand, in the sphere of European integration, how the European Union affects and influences its Member States in the formulation of measures related to the cybersecurity of its citizens. Hence, Portugal will be used as a case study. This choice stems from the fact that this country contains an unexplored volume of academic literature regarding the topic, in comparison with other larger ones. Therefore, the main objective of this work is precisely to provide a new view on how the EU has shaped the legislative process of a small country, but important nonetheless in its position on the European panorama.

Keywords: Cybersecurity; Europeanization; Portugal; European Union; Internet

Index:

Glossary of acronyms:

CERT - Computer Emergency Readiness Team

CNCS – Portuguese National Cybersecurity Centre

CNPD – National Commission for Data Protection

CSIRT – Computer Security Incident Response Teams

DSP – Digital Service Providers

EC3 - European Cybercrime Centre

EDPB – European Data Protection Board

ENISA – European Union Agency for Network and Information Security

EP – European Parliament

EU – European Union

EUROPOL – European Union Agency for Law Enforcement Cooperation

FCT – Foundation for Science and Technology

GDPR – General Data Protection Regulation

GNS - National Security Office

ICT – Information and Communication Technology

IoT – Internet of Things

ISP – Internet Services Providers

MS – Member State

NCSSs – National Cybersecurity Strategies

NIS – Network and Information Systems

OES – Operators of Essential Services

PJ – Judiciary Police

QNRCS – The National Framework of Reference for Cybersecurity

SME – Small and Medium Enterprises

WG – Working Group

Introduction

Every 39 seconds, there is a new cyber-attack[1]. Our dependency on information and communication technologies (ICT) has grown according to our need of having these services more present and effective in our social activities. Even though they facilitate how essential information circulates throughout the world, they also pave a way for crime to become elusive. As it happens, the bigger the demand of these products is, the higher the risk of compromising security: data theft, hacking, cyber extorsion, cyberterrorism, among others, are gradually becoming a reality in user's daily activities, harming not only citizens, but also corporations and government institutions. Therefore, cybersecurity is becoming an area of study more relevant in the past years and is getting positioned at the forefront of political agendas (Wessel, 2019; European Commission, 2018).

The European Union (EU) has interpreted Cybersecurity as a continuous process that requires the constant communication and cooperation among all the Members States (MS). One example is how this subject has accordingly pierced in the most recent State of the Union speeches (ibid.), and has asked for a stronger certification framework, taking in consideration the changes in the "technological and security landscape" of the Union (European Commission, 2017: 1). The urgency in building EU resilience seeks to oversee the necessity of the MS, but to assist national governments, vendors and providers, as well as citizens and end-users (ibid.).

Likewise, the aim of this work is twofold: to study the European Union's policies regarding Cybersecurity applicability – fusing the concept of Europeanization as an analytical tool for European integration among its MS; and focusing on the case study of Portugal and the process of law-making in combating cybercrime and establishing cybersecurity methods. Although each Member State has their own way of tackling this problem, as this policy field is still an exclusive competence thereof, they all respond the EU and its ruling institutions, in order to enhance collaborations and exchange of information to attain a response to incidents – especially with the implementations of national Computer Emergency Response Teams (CERT's). Portugal is no exception. And

[1] Security Magazine, (2017). *Hackers Attack Every 39 seconds* [online] Available at: https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds [Accessed: 19 Mar. 2020].

while it is still one of the most victimized countries in the EU concerning cybercrime[2], it has recently been adopting newer and better defence regulations. However, this process has not been stable, but rather irregular and lagging (Silva, 2019).

While the EU has asked for a stronger and firmer development of national operations with the main role of conducting cybersecurity strategies (European Commission, 2013), Portugal has only started implementing European legislation in recent years (Silva, 2019). Even though the National Committee for Data Protection was established in 1991, the urgency for better regulation came at a time where other Member States were also starting to implement new measures. Transposing the Network and Information Systems (NIS) Directive – in 2018 – into Portuguese law, embedding the General Regulation on Data Protection (GRDP) in the same year, and creating the National Cybersecurity Centre, in 2014 – working as the main authority for Cyberspace-related matters – were the major advances regarding this field of action taken by the Portuguese government. It is important to accentuate that all these examples happened during the last ten years (in the moment of the writing of the present dissertation), and more developments are likely to come to fruition in subsequent years.

In order to participate in an EU-level dialogue, Portugal is still examining how new cybersecurity policy can affect the country's political, social and economic stance: an issue that it is still happening while this dissertation is being written. The issue of cybersecurity has been gaining relevancy (Carvalho, et al., 2020) with the exploration of the cyberspace and the exponential growing threats that come hand in hand with emerging technologies.

Even though the EU has long developed technological changes regarding the accessibility and the security of online communications (Council of the European Union, 1997), the growing number of cyberattack incidents, as well as their complexity, detected in the last decade, raised concerns among the MSs and made the EU rethink how cyberthreats needed to be addressed (Carrapico & Barrinha, 2018). The core of this mindset change came also at a time where national governments were dispersed and leaving various actors working on the lure and autonomously from each other (ibid.). Consequently, the need for a common policy was important to face newer challenges on multiple dimensions and to act on different contexts.

[2] European Commission, (2015). *Cyber Security Report*. [online] Brussels: Eurobarometer. Available at: https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf

We will begin by going through the most relevant available scientific literature to provide an overview of the concept of Europeanization, which we will use to analyse the EU's position as an agent for implementation of common Cybersecurity policies among its Member States, with a focus on Portugal. In the literature review, we will go through the multiple approaches and lines of thought and we will critically examine the latter and identify a specific conceptualization to carry out our analysis. In the subsequent chapter, we will provide the methodological choices for the dissertation as well as a proper justification of the case study and timeframe, taking into consideration the research questions and principal objectives.

Methodology

In order to evaluate the impact of the process of Europeanization itself and the field of Cybersecurity, the research question presents a descriptive nature and it is the following: how has Portugal responded to Europeanization, in terms of "domestic adaptation to the pressures emanating directly or indirectly from EU membership" (Featherstone, 2003: 7), in the policy field of Cybersecurity, during the period ranging from the establishment of ENISA to the implementation of the Cybersecurity Act?". To properly answer the question, a qualitative method will be used for this type of work, as its main objective is to describe the complex process of Europeanization.

By doing so, Europeanization will go in hand with the research process of this dissertation, as it will be used as a key concept to analyse the EU's influence on its Member States in the policy field of Cybersecurity – in which Portugal will be used as a study case later on. However, there is a distinctive difference between European integration and Europeanization: while the first one emphasizes the sovereignty of an entity to a supranational organization – in this case the European Union -, the second definition usually refers to an instrument in a larger European integrational context (Radaelli, 2004). Likewise, political integration has been a wide subject of research, putting such actors like the EU in a position of shifting the dynamics on law-making in order to create a "new centre, whose institutions possess or demands jurisdiction over the pre-existing national states" (Haas, 1958: 16 in Graziano & Vink, 2013: 32). Portugal's legal composition goes along this notion and opens space for a broader dialogue: where there has been a lack of consensus, there is also been recently several attempts to

correspond to today's challenges and tackle growing cases of cyberthreats (Carvalho et al., 2020).

In the second part of this dissertation, we will explore the EU's position on Cybersecurity and the methods of political and technological integration. Even though this is a long and many-sided process, it is important to set a time frame for our analysis, starting from the creation of the European Union Agency for Cybersecurity (ENISA), in 2004), to the implementation of the Cybersecurity Act, in mid-2019, that created the first-ever certification for EU-CERT's. For this part, we will also analyse a series of primary sources, such as annual reports by ENISA, as a way of detailing the evolution of the Agency in providing assistance to the MS, but also official regulations and directives by the European Commission and the European Council, to demonstrate the "meaning of the document and its contribution to the issues being explored" (Bowen, 2009: 33) in the field of cybersecurity. Other miscellaneous sources will be added to the analysis for support, including reports made by the European Council for Foreign Affairs, news reports, and other material found in official websites – most significantly – ESC, the European Cyber Security Organization, prearranged as an "industry-led contractual counterpart of the European Commission for the implementation of the Cyber Security contractual Public-Private Partnerships (cPPP)" (Gruber, 2018: 9).

Secondary sources were also specifically picked as a way of providing a better insight on the topic and balancing information alongside the primary ones: some of the examples include academic literature and reports from the European Court of Auditors.

Since this dissertation is heavily relied on document analysis, as an important tool to gather information, the third part of this dissertation will be essentially focused on the case study of Portugal. Like it was previously mentioned, it will analyse legal documents, mostly provided by the Portuguese government – such as Resolution of the Council of Ministers, reports from national Ministries, among other –, as a way of congregating more precise data. However, in this chapter, it will also include interviews, most notably directed at members of the National Cybersecurity Centre (CNSC), bridging how EU regulation is implemented in Portugal, and experts in cyber strategies, especially journalists that work within the field. The objective of conducting interviews is, on one side, to add a more human touch to the discussion and, on the other, for being a model that allows us to make direct and follow-up questions. All in all, the usefulness of EU legislation will be put to test, as to see how much of it applies and involved Portugal.

Chapter 1- State of the Art

1.1- Theorizing and Framing Europeanization

Europeanization has been described as a chameleonic term that has stored throughout the years various definitions, while also undergoing a constant transformation (Ladrech, 2002), and taking in consideration the inherent phenomena that happens adjacently – which opens the debate for its use as an "organizing concept" (Olsen, 2002: 922). However, the topic comes to the surface when talking about European Studies and gains importance when confronting the role of European Institutions. It is inevitably a concept with history – one that encompasses multiple layers.

Johan P. Olsen attends to those layers in his definition of Europeanization (2002: 923-924). In his view, Europeanization is identified when it comes to "changes in external boundaries", as an extension of policies, rules and internal requisitions by the new added states. The process is, however, continuous and includes other courses of action that the author explicitly points out as being "developing institutions at the Europe level", penetrating "national systems of governance", "exporting forms of political organization" and uniting "political projects". All of these help in promoting capacity building and domestic adaptation at the EU-level.

While Olsen's definition provides an outlook of Europeanization as "model-building puzzles" (Radaelli, 2004: 3), illustrating the different components of its unification and integration processes, it is constituted simultaneously by two greater understandings that are based on Bulmer's (2008) work: Europeanization not only translates EU matters to other jurisdictions, but also handily builds organizational capacity as a whole. Radaelli (2004) compliments Olsen's work; yet, points out how it can also lead to a broader and disheartening interpretation.

In his view, Radaelli (2000.) shows the importance of EU's social, political and economic dynamics to become a permanent reality in domestic political structures and public policies. It is, however, important to notice how his definition stresses behavioural changes and not organizational ones: it encapsulates social construction and institutionalising processes, while at the same time referring to its nature of incorporating EU formal and informal rules (Radaelli, 2004: 3) – showcasing Europeanization as an interactive process, not a discriminatory nor a unilateral one. The conceptions of Europeanization that Radaelli works with, described as an adaptational design, are very

helpful in showing Robert Ladrech's take on the subject. Most efforts involve identification of appropriate levels of analysis, but, in its widest meaning, Ladrech sees it as a "response by actors to the impact of Europe integration" – one that happens at an increasing level. (Ladrech, 2002: 389).

For both an internal and external interpretation, Europeanization defines and redefines different ways of identification for both territory and people. For Borneman and Fowler (1997), Europeanization truly started post-World War II between the United States and the Soviet Union as a way of positioning Europe as a leading figure of the international scenario. While being less substantial than most of their colleagues, the two authors are the only ones in the identified scholarly debate that call for a pan-European statehood and peoplehood: the capacity for the EU to invoke the principle of territoriality to fortify the ability of members to organize space and to direct historical remembrances from both national and continental perspectives. Their insights seem to come from the point of view of outsiders: two Americans studying European phenomena at the end of the 1990s: a period marked by numerous geopolitical actions inside the EU[3]. For Borneman and Fowler (ibid.), the terms of political organization are moulded according to the nation-state model, which bridges territorial formation with populational organization.

Even though their article focusses on the role of states as figure forms with strong statehood politicized with the objective of politically and ethnically unifying mixed and dispersed populations (Borneman & Fowler, 1997), the debate on the role of the nation-state still remains alight. Tömmel's (2014) analysis is much more substantial as her point of view balances itself throughout diverse academic backgrounds: she takes Majone's (2005) definition as a way of meeting the former authors' position of the EU as set of "corporate bodies balanced against each other governed by mutual agreement" (Majone, 2005: 46 in Tömmel, 2014: 23)[4] to conclude that the EU is defined by a political system that goes beyond the nation-state. It is built on particular establishments that represent not only the nation-state, but the people that establish such notion, taking into consideration as well the interest of the Union as a whole. In her thoughts, the EU is a "dualistic, bi-

[3] europa.eu, *The History of the European Union – 1999*. [online] Available at: https://europa.eu/european-union/about-eu/history/1990-1999/1999_en [Accessed: 25 May. 2020].

[4] Majone, G. (2005). *Dilemmas of European Integration: The Ambiguities and Pitfalls of Integration by Stealth.* Oxford: Oxford University Press.

cephalous political system" (Tömmel, 2014: 26): a hybrid organization that takes in both supranational and intergovernmental institutions.

Within the chosen literature, there is little mention made of the role of political parties identified as actors. However, Ladrech splits it into two fields: a first part more linked to party activity groups in the European Parliament (EP); and a second one that pays closer attention to European "policy orientation of individual political parties" (Ladrech, 2002: 390). According to the author, Europeanization does not constitute an answer to European integration by analysing political parties as organizations, but through cooperation among parties between Member States. Political parties are limited in their response to EU integration, especially regarding national policy making. Still, the increased significance of the EU impacts on domestic policies, but never only from one side. There is no institution that can particularly weigh the responsibility for EU issues, since the EU as a regional integration organization is involved in so many policy areas. Hence, the author argues that Europeanization is seen as an all-embracing process of responses by parties that open space for various and possible actions (Ladrech, 2002). The environment is constituted by a series of scenarios that powers change, in the sense that external inputs dwell into the behaviour and structure of domestic political systems. Overall, theorising Europeanization should not present itself to political parties as an insoluble hindrance within the regional determination (ibid.).

1.2- The Domestic Impact of the EU

Europeanization can be described as a cause in the search of an effect at the domestic level (Goetz, 2000). While authors like Schimmelfennig (2015) still consider if there is a possible and functional process of Europeanization going on, it is decisive nonetheless to trace its movements and historical processes. For decades, the accountability of emerging EU policy was debated between neofunctionalism, "a special variant of functionalist approaches", and intergovernmentalism, grounded in the theoretical tradition of neo-realism approaches (Tömmel, 2014: 2). Since the late 1950s, comparative politics and International Relations theories worked as the foreground. These two early theories battled each other and seemed to purposely conclude where the other one was missing. Tömmel (2014) puts them in perspective: while the former developed the progress of the EU as an institution, emphasising the internal dynamics that drove integration, the latter addressed international organization in general.

Graziano and Vink (2013) go further – through Moravcsik (1994) – in proving that intergovernmentalism put to test both the empirical and theorical notions of neofunctionalism: not only do they defend that neofunctionalism increased the misunderstanding of trajectory and purposes of the European Community, but also lacked the theoretical background in providing a sound basis for "precise empirical testing and improvement" (Moravcsik, 1993: 476 in Graziano & Vink, 2013: 32)[5]. Hence, intergovernmentalism emphases on the role of 'rational' governments that can consequently work and negotiate at the EU level.

However, neofunctionalism was built upon the assumption of international cooperation. The core concept actually circled the mechanism of spill-over (Tömmel, 2014), as a form of integration at an initial matter that triggers greater integration as a result of functional needs. Haas (1958) was a crucial figure in the constituents of neofunctionalism, defining political integration as:

> "The process whereby political actors in several distinct national setting are persuaded to shift their loyalties, expectations and policial activires toward a new centre, whose instituitions possess or demand jurisdiction over the pre-existing national states" (Haas, 1958: 16 in Graziano & Vink, 2013: 32)

It is important to notice that the transference of policy areas and functions is not an automatic nor a pre-determined process. On the one hand, neofunctionalists defend the primarily role of national governments and political elites to recognize the advantages of implementing related policy areas and to progressively advance the process of integration. They argue that the more functions are transferred to EU-level determinations, the bigger will be the number of political parties, interest groups, and international associations to shift their activities to the same level (Tömmel, 2014). According to Graziano & Vink (2013), the advancement of integration is made through the loyalty expressed by non-state elites that have considered a new European supranational setting to be in line with the joint group of preferable social and economic preferences. The notion that non-state actors may be fulfilled by their search of European integration is beneficial mostly to their selected interest and respective backgrounds.

On the other hand, intergovernmentalism proposes that international integration would only materialize within states through cooperation (Tömmel, 2014; Bulmer, 2008). Integration moves forward when actors' interests converge, just like when different

[5] Moravcsik, A. (1993). *The Choice for Europe: Social Purpose and State Power from Messina to Maastricht*, Ithaca, NY: Cornell University Press.

interests are adjusted to an agreement. By that, intergovernmentalism succeeds when integration can be explained over a series of bargains: partial transferences among national governments at the EU-level in order to create institutions for decision-making. Moravcsik was an influential figure that linked national governments' strength with the need for a wider, more collective and integrational procedure (Bulmer, 2008). Bargaining subsequently has been very much present within intergovernmental analysis; however, usually with a negative connotation. Börzel and Risse (2009) categorize it as a strong asset among powerful member states, as it displays a bigger difference when talking about European integration. Countries like "Britain, France and Germany" are unlikely to face a significant period of change when in comparison with other members.

Börzel portrays the impact of Europeanization as a two-way process: "bottom-up" and "top-down" (Börzel, 2002: 193). These two methods are a key element to document the European process of penetrating at a domestic level in a way that can open the floor for various discussions. While Graziano and Vink (2013) affirm that Europeanization should not be classified as a top-down domestic adaptation directly from the EU – but a relative learning development of informational decision making and diffusion –, in a retrospective approach, Radaelli (2004) highlights its relevance during the 1970s, and 1980s, but also its presence in current research projects as a way of detecting the implementation of European policies.

To Radaelli (ibid.), Europeanization is about governance: an ensemble of mechanisms made to measure the power of European integration by establishing, for example, the idea of partnership between private and public actors and by inserting multipart layers of governance in the regions. According to the author, the remaining question is to fully understand whether or not the EU is producing a legitimate form of governance or simply presenting different versions of existing forms of governance (ibid.: 6).

To the author, it is undeniably relevant to understand Europeanization as a process of governance; still, some authors add a second explanation, one that links it to Institutionalism: a theory born in the 1990s that more precisely says that the function of integration does not depend on the pragmatical choices and decisions made by the members states (Börzel & Risse, 2009). March and Olsen present the role of institutions

in the political landscape (March & Olsen, 1989 in Tömmel, 2014)[6]. According to Olsen (2002: 932), the framework of Europeanization is well-intended throughout "experimental learning" and "competitive selection". Change here is the premise and it is used as an analytical tool to further investigate how European-level developments penetrate the domestic level and produce an impact. The first one relates to change "on the basis of experiences with, and interpretations of how relevant actors in the environment respond to alternative forms of domestic organization and governance", while, on the second one, "environment imperatives are seen as driving the change process, and there is a need to understand mechanisms of variation, selection and retention" – as a way to finding how well institutions and actors match their normative settings (ibid.: 932, 933).

But like Olsen (2002) indicates, adaptation can be constructive and its processes do not always work accordingly. The adaptability proportion may be irregular to the change in the environment to which the institution is adapting. EU policy-making can expect various and differentiated patterns and responses, partly, because EU influence in institution-building can unevenly develop across policy areas, which means that the pressure certain states and institutions face may vary.

Olsen (ibid.) affirms that the extensive event of piercing domestic-level institutions by the EU is happening in unregular stages and by that it is important to attend to how differently Europeanization might impact the Member States, since certain governments need to adapt to European pressures in their own ways.

> "Europeanization as domestic impact is not limited to structural and policy changes. European values and policy paradigms are also to some (varying) degree internalized at the domestic level, shaping discourses and identities. Europeanization of foreign policy has produced a shared norms and rules that are gradually accumulated, rather than being a process where interests have been fixed" (Olsen, 2002: 935).

While Olsen (ibid.) works with two process that justify the EU's agenda for integration, Schimmelfennig (2015) distinguishes new mechanisms categorized by two different dimensions. Considering Bulmer's work (2008), Schimmelfennig (2015) defends that Europeanization can be achieved by EU-driven policy or by institutional implementation, following the logic of consequence or the logic of appropriateness. According to the

[6] March, J.G & Olsen, J.P. (1989) *Rediscovering Institutions: The Organization Basis of Politics*. 1st edn. New York: The Free Press.

author, in the first, Europeanization can be attained by the EU through sanctions and compensations that directly or indirectly affect the economic relationship of the target state (ibid.). These incentives not only give the EU credibility as a motivator, but also make the target state achieve such requirements. The latter is works lustrously as a social construct, a social learning. The states that are looking forward to EU influence are persuaded to such ends; however, only if they identify with the EU at some level. The regulations here are implemented through transnational mechanisms via societal actors – or by 'bargaining', as mentioned earlier, in intergovernmental relations (ibid.).

The relationship between the two may be irregular, like the author attests. Still, the position of discontent some non-member states express with their domestic reality can make them pursue EU rules as a problem-solver, "either based on instrumental calculations or appropriateness of the EU solutions" (ibid.:7). But the process of resolving a Member State's problems falls under the reality of EU integration and external governance to which intentional action of the EU may trigger adaptation complexes. This fact alone opens a new dialogue in the literature as a way of dictating how this process may work itself out. The EU's way might offer a model for other regions and outsider social actors to perform under. But by doing so, as Schimmelfennig (2015) argues, this positions the European Union as a 'model for presence': a result of its influence and capacity as an important system regulator. To Radaelli (2004), it counts as an exercise of governance, but one that can be reached by means of 'goodness of fit' and 'misfit'. The 'misfit' idea claims that, in order to achieve domestic change, the process itself needs to be uncomfortable and stressing for the institution – experiencing at the same time more external heaviness. It opposes the 'goodness of fit' in a way that the latter depends on lower adaptational pressures on national institutions, opening space for a set of clear developments of rules and practices from the EU (Risse *et al*., 2001: 7 in Graziano and Vink, 2013: 41)[7]. Bulmer (2008.) defends the hierarchical (or "top-down") context of such terminology, while Graziano and Vink (2013:40) discard any possible linkage to a theoretical status in Europeanization studies, since "it is more concerned with domestic political change rather than EU political development".

[7] Risse, T., G.C, M., and Caporaso, J. (2001). *Europeanization and Domestic Change*, Ithaca: Cornell University Press, 1-20.

However, it is in Bulmer's (ibid.) findings that a new interpretation gains form, as his analysis is well-rooted in European Politics[8], proving an accurate perspective on academic literature regarding EU matters. Conferring his approach, EU requirements for adaptation are mostly unbalanced insofar as the relations in question are formulated: the adjustment pressure is not the same between member states and it is justified by the implementation of veto points or by supporting facilitating formal institutions at a domestic level. It ends up depending on the level of "commixture" domestic actors may be able to secure adaptation, serving as a consequence a differential impact of Europeanization. (ibid.).

Bulmer (ibid.) acknowledges nevertheless the prominence of the 'fit/misfit' framework; still other theoretical reference points have emerged from studying policy formulation. Even though the author's understandings are rationalist in nature, forestalling how domestic actors will respond to institutional changes, Börzel and Risse (2009) chose to adopt new variables associated with sociological institutionalism. Consequently, domestic actors can undergo social learning even to the extent of developing new identities, emphasizing on a cooperative political culture as a strong mediating factor.

Both higher or lower degrees of misfit potentialize responses to Europeanization, which can be identified through time, whether it be in the short or long term. Börzel and Risse (ibid.) recognise three different forms of domestic change: Absorption, Accommodation, and Transformation. Three examples that document the process of integration regarding adaptational pressure. Absorption houses EU ideas into the programmes of the Member States without getting to a phase where it substantially modifies existing policies and institutions. Accommodation incorporates EU ideas without changing essential features: a way of doing so is by "patching up" already existing policies, new models, and ideas without jeopardizing the collective understanding of the community. Finally, Transformation is where the integration rate is higher. The Member States replace existing policies with completely different ones, causing a major change in the political panorama nationally (ibid.: 14).

The authors developed these theories in 2009, and, even though they would have been more compelling if presented alongside practical cases, they still remained relevant

[8] speri.ac.uk, *Simon Bulmer, Professor of European Politics, Department of Politic* [online] Available at: http://speri.dept.shef.ac.uk/people/simon-bulmer/ [Accessed: 8 Jun. 2020].

throughout the years. Four years later, they are still ingrained in Graziano and Vink's (2013) approach. According to the authors, the EU is not causing any convergence directly between the Member States, since the impact of such an organization with great governance is already arbitrated by pre-existing domestic factors that balance the way in which the EU uses its powers (ibid.). However, the authors claim that Europeanization goes beyond legislative matters – it touches the action of political parties, provides political opportunities for non-instructional actors, affects interest groups and social movements, and so on (ibid.).

Despite the increasing EU-implemented changes in the functioning of domestic actors, both Graziano and Vink (2013) and Börzel and Risse (2009) agree that Europeanization is not a model for convergence; in fact, the authors argue that the two should not be considered synonyms. Such conclusion is due to the notion that "convergence" is considered a loose term, especially because of how ambiguous its interpretations can be: what looks like convergence at a broader level may still show a significant degree of divergence at a narrower level, and vice-versa. While convergence can be achieved in political outcomes, it is partial and in regard of instruments, politics and policies:

> "EU rules and regulations require convergence in policy outcomes […], while they leave quite some discretionary power to the member states with regard to the means how to ensure compliance. Thus, we need to specify what we meant by "policy convergence", convergence in outcome (which equals compliance with EU law and, thus, is not particularly interesting to observe) or convergence in policy processes and instruments" (Börzel and Risse, 2009: 16).

Radaelli (2004) takes a similar stance to the previously mentioned authors. As formerly mentioned, Europeanization can be identified as many forms of governance, discourses, and through various aspects of institutionalism. However, it cannot be categorized as convergence. States respond to the opportunities and constraints provided by Europeanization, but always according to their structural characteristics. This conception helps in showing the arbitrary nature of convergence, as it is difficult to mediate it across Europeanization. Radaelli (ibid.) confirms this idea by affirming that the same country can respond differently depending on its actors and available resources in different policy areas. In theory, convergence can indicate a shared language, but not in an isolated and imposed manner. The author demonstrates that the EU's models have not properly converged in years. And even when they did so, it was not through a "top-down" process, but thanks to the outcome of domestic political decisions (ibid.: 14,15).

Europeanization processes are constantly in motion, just like the domestic adaptations to them. It is possible to conclude that Europeanization is not a new conceptual approach, but one that is undoubtedly crucial to the study of Political Science. The framework proposed by the identified literature mostly does not break ground on a drastically domestic change, but instead proposes an open interpretation to enable more empirical research results. It is relevant to admit that Europeanization has provided new analytical tools that study the dynamics of the EU's complex political system; and overall, most authors agree that the future challenges new meanings for Europeanization, becoming even more promising on growing regional integration research plans.

1.3- The EU's measures in creating cybersecurity policy

The European Union has been developing, for the past decade (at the time of the writing of this dissertation), new activities related to computer security and electronic communications. Cybersecurity has, in fact, transformed into a common bullet point in the EU's narrative and has been adapted to Academia as a subject of in-depth research. Most authors agree that a shift in the European Union's discourse happened thanks to the modernization of our daily lives, and likewise scholars followed accordingly (Ruohonen et al., 2016). While the internet became an omnipresent entity, the emergence of cybersecurity came as a major issue of international security. Rapidly, threats such as cyberattacks developed into an imminent and unprecedented phenomenon.

Ruohonen et al. (ibid.) argue that an effective and innovative approach comes from setting two major goals: first, a scholarly one, more based in theoretical viewpoints, and second, a practical one, leveraging institutional change. Traditional International Relations and Political Science schools of thought have been outdated when it comes to cyber matters: not only because their progressive and irregular structure, but especially because conventional theories conceptualize this issue in different boxes: as a private, military, or civil one (ibid.). However, the authors open the discussion regarding institutional change, one that is either incremented or abrupt. To them, the result of such change can vary according to processes of continuity or discontinuity. According to the authors, by focusing on empirical indications of institutional modification, change in theory can be accomplished and can result in disruptive transformation – especially when changes are portrayed against the historical evolution of the respective institutions. Many

cybersecurity matters, like the Conficker Worm[9], for example, were solved thanks to network coordination between public and private sector actors (ibid.).

This change however was not sudden nor revolutionary: it appeared as a model of adaptation for a new, political, and technological situation analysis. The entry of the European Union in the cybersecurity course of action caused a viable change in the organization, starting by creating a cybersecurity apparatus that was built, according to the authors, upon "an informal but largely technical, engineering-driven, governance system between various national teams responsible for network and computer security" (ibid.: 747). The creation of European Computer Security Incident Response Teams (CSIRT) has followed a linear trend since the 1990s, in order to reinforce coordination among the EU. The CSIRT's initial attempts, however, failed as national teams refused to incorporate the "top-down" tactics that were initially planned. Later, a network body for EU-CSIRTs was put together in the 2000s. While this specific body was created to cement a better integrational procedure, the perspective the authors takes on points into an unsure and restrained beginning.

Going back to the existence of insufficient studies on this issue in particular, most authors agree that there is still a military-oriented nature to them – mostly relating to security measurements (Rid, 2011). And while Ruohonen et al's (2016) approach is hopeful for a near future, Cavelty's (2018) showcases the difficulty of grasping such new concepts without a proper systemic analysis of the topic. According to the author, a concrete body of literature on cyber-power exists in minor proportions and its generally politically biased to a clear dominance of US military forces or by other strategic voice. The author sustains a non-existing, but rather important, debate about the differences and principle features of cyber-power, shedding a light also on the notion that there is no further discussion about the growing relevancy of cybersecurity policies (ibid.). While Cavelty's (ibid.) work is more accusative, Christou's (2018) article is much more substantial to the work of international organizations, notwithstanding derailing from Cavelty's premise. They both agree on the importance of studying cyber-power conceptually or normatively, and how sometimes IR theories lose too much time conceptualizing it. They are both on the same page regarding EU interpretations not being equally developed among MSs ("Not under the same name" [Cavelty, 2018: 305]).

[9] Bowden, M. (2019). *The Worm That Nearly Ate The Internet.* [online] The New York Times. Available at: https://www.nytimes.com/2019/06/29/opinion/sunday/conficker-worm-ukraine.html [Accessed: 11 Jul. 2020].

However, Christou goes deeper into the components of internal security organizations and displays a series of examples, like poorly trained professionals, limited tools with regard to information sharing, unequal forensic capacities across the EU or an inconsistent assistance among participants in cybersecurity (European Commission, 2012: 3 in Christou, 2018)[10]. His article is the only one that we found that tackles these challenges in a way of documenting the struggles of the EU, but also its solutions. With the creation of new models of governance like the Joint Cybercrime Action Taskforce (J-CAT) located within the EU's European Cybercrime Centre (EC3), based in the Netherlands, Christou sees a more functional vision for the EU cybersecurity environment (Christou, 2018).

The identified scientific literature converges in detailing a single year as a vital turning moment for the EU's cybersecurity policy, namely 2004, with the establishment of the European Union Agency for Network and Information Security (ENISA), the first EU specialized in network and information security that assists Member States with their own national cybersecurity strategies (NCSSs) (Sliwinski, 2014; Markopoulou et al., 2019). Sliwinski (2014) brings attention to ENISA having concluded throughout the years, that without a national cooperative institutional body, the EU will never have an effective response to cybercrime and other cyberthreats. In fact, citing data from the Agency, the author sustains that 12 of the 27 Member States do not have dedicated cyber strategies, which makes them rely on "national security strategies" (ibid.: 470) at best. Still, the author highlights the superlative approach that this EU institution has in attending to the MSs necessities with assistance and technical advising. The task of ENISA comes from a place of constant communication and regulation with the EU Member States, always with the objective of raising "awareness of network and information security and to develop and promote a cultural of network and information security in society for the benefit of citizens, costumers, enterprises and public sector […]" (EP and the Council of the EU, 2013: 48). Still, there is not a specific take on the role of ENISA as a catalyst for positive or negative regulation among the authors, since it is still a work in progress.

From 2010 to 2019, there have been calls for an enhancement of ENISA's mission to implement better security policies between the Member States – now with greater urgency

[10] European Commission. (2012). *Communication from The Commission to The Council and The European Parliament: 'Tackling Cybercrime in our Digital Age: Establishing a European Cybercrime Centre'*, COM (2012) 140 final, Brussels, 28 March 2012.

thanks to the new Cybersecurity Act. Markopoulou et al. (2019) have stated in their article that ENISA is the only EU agency with a "fixed-term mandate", that ends up limiting how they sustain their participatory actors, looking at the same time for a stable-footing in the future. The general ICT framework still remains optimistic, as the authors take a less critical position and admit it to be a trustworthy key for the European Union to achieve their goals in response to cybersecurity (Markopoulou et al., 2019).

Since ENISA's establishment, progress has been recognised in methodical and political levels: cybersecurity is now listed as one of the EU's most important priorities, and transversal elements related to it have been integrated within other EU policies. However, it is still relatively new territory, one that causes divergences. For Sliwinski (2014), the EU has remained relatively formative policy actor when compared with other countries, such as the United States or China. In addition, even though the author points out positive reinforcements in the EU's cybersecurity policy in recent years, its limitations are the most pejorative factors so far. Sharing this position – which appears to be a prominent point of view within the scientific literature –, are Markopoulou *et al*. (2019). From 2013 to 2015, the Commission, the Council, and the Parliament opened dialogue for NIS Directive, the first "horizontal legislation" launched at the EU-level that was implemented in August 2016 (ibid.). While it was identified as a vigorous and vital response that takes into account the protection of network and information systems in a more assertive manner, the authors highlighted the lateness of such response and how, by time the NIS Directive was executed, the ground rules for cyberterrorism counterattack demanded bigger attention.

On a similar note, Christou (2018) follows a similar argument, describing the NIS Directive as a 'controversial' measure in a way that overlaps the critical and primordial role of the EU's policy for creating a safe infrastructure, as well as the EU's role in dealing with cybercrime.

The form of legislative act made all sectors report data breaches across all operators of essential services; it also dealt with non-legislative matters in a secretive and non-transparent way: something that made many EU-CSIRTs uncomfortable and confused, mainly because the Commission's strategy was promised in a context that prioritized "dialogue, partnership and empowerment"[11].

[11] Commission of the European Communities. (2006), *A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"*. [online] The European Union. Available at: https://ec.europa.eu/information_society/doc/com2006251.pdf [Accessed: 12 Jul. 2020].

The European stance regarding cyber-power comes from a place of mutual connection and central agreement within the Member States. Cavelty (2018) deconstructs this notion as a shared-value of common resources that work with the objective of creating and controlling electronic and computer-based information: a set of networks, infrastructure and human knowledge that fluxes without constraints nor restrictions among the members. The EU's approach is based on maintaining a multi-level governance model in the terms of political and economic interests and assets of the World Wide Web. Decision-making goes hand in hand and it is much more approachable when actors and lobbyists interact mutually in a way that benefits the EU (ibid.). With this, the EU's cybersecurity strategies are presented by "technical risk management strategies, standardization of methods and concepts, harmonization of law and attempts to achieve better coordination" (ibid.: 313) among the previously mentioned participants. This notion of common responsibilities that Cavelty (ibid.) mentions constitutes an unbalanced political reality: in her work, while the EU strives to make sure full coverage of network security is transnational, her realist perspective shows that cybersecurity practices mirror inequalities, since the EU indulges itself in its need to secure and protect. The author later concludes that most of the member countries struggle with protecting their networks, depending on their own capacities and available tools (ibid.).

Carrapico and Barrinha (2018) circle around what Cavelty (2018) states in her article, but they end up being more articulated and precise. They enumerate examples that justify the present state of cybersecurity in the EU, presented as challenges, both internal and external, that augment such disparities. The absence of public awareness and relevancy of cyber terms and emerging concepts, the complexity in creating and distributing efficient tools to commit cybercrime, the lacklustre capacity by the private sector to attend to incidents – met as well with an unwillingness to invest in protection devices – are some examples that the authors pay special attention to. However, like most of the previous authors, it is possible to extract a positive outcome from their article. The EU's effort has been reinvigorated by the promise of cooperation, greater involvement in public and private sectors and investments in cyber defence capacities. The already announced enhancement of ENISA's abilities and the creation of an official cyber security certification for services and providers to support the Digital Single Market are some of the prospects for the future that Carrapico and Barrinha (2018) mention.

There is a convergence among the identified scientific literature regarding the usage of terms like "cooperation", "cyberspace", "cybercrime", "lack of consensus",

"infrastructure", "essential services", "Digital Single Market", among others. Some concepts, conversely, have a short life expediency, becoming, through time, reinvented. The notion of "cyberwar" is one of them. While it has still maintained an evolving, crucial, and disciplinary meaning, it was quickly detached from its original interpretations and symbolisms, within the context of international conflict (cf. Rid, 2011 and Stone, 2012).

Cyberwar is more predominant in early research, because just like cybersecurity as a whole, it fitting can be included in various categories. Rid (2011) and Stone (2012) argue over their relevancy as the all-pervading nature of the internet strengthens. For the former, cyberwar seems like a distant present, one that probably will not materialize because of its man-made leanings. The latter connotates cyberterrorism as a mechanism for war, since it can negatively influence the *zeitgeist.*

For the EU, the looming preoccupation with cyberthreats developed into prevalent concern in addition to search, within this policy area, for institutional and policy coherence – a goal that Carrapico and Barrinha (2018) argue is the cornerstone for future advancements and a fundamental aspect for relevant actors to stop working independently from each other. After the enactment of the Cybersecurity Act, the EU General Data Protection Regulation (GDPR), implemented in May 2018, was seen as the next big step in EU cyber protection, aiming to bring a single standard for data coverage among all EU Member States. But again, much like the topics that were previously covered in this section, the "novelty" factor seems to be only restrictive.

When searching for scientific literature, most of the readings are placed within the field of computer science and/or computer engineering, areas whose technical knowledge is not accustomed and accessible to all. By comparison, there is still work to be completed in the scope of IR on how cybersecurity is being transversally integrated into political and social life. Markopoulou et al. (2019) write hopefully of the GDPR, as a powerful vehicle for individual rights in all things digital, but still casts doubt on its position among prior cybersecurity actions, such as the NIS Directive, and mirror them in terms of accountability and performance results. The two law making documents were launched as a way of dealing with data, founded either on systems of digital service providers or operators of essential services. However, there are contradictions in the authors' words, as they admit that both legal instruments need to be "listed separately" and "judged independently, each for its own merits" (ibid.: 10), while also specifying that the lack of acknowledgment that covers the two does not mean that they are "unrelated", as "both

legal instruments find application at the same time" (ibid.:9). They conclude that being cybersecurity a field of global regulatory interest, the GDPR and the NIS Directive have attracted such substantial amount of attention that the authors believe it to be "unwarranted". The point of both systems is not supposed to contradict one another, but to balance each other out, pursuing the solidification of the Internet as a parallel universe:

> "Notwithstanding therefore the contemporary GDPR prevalence and ever-presence […], we believe that even on the few issues where the two legal frameworks intersect, one ought to leave the other largely unaffected, each security measure, personal data breach or incident being judged separately under its own circumstances" (ibid.:11).

The particularity of Markopoulou et al. (2019) lays on the notion that the NIS Directive is permanently at the forefront of this discussion, making elements such as the GDPR, the Cybersecurity Act, and ENISA never actually individually analysed. For a more quantitative analysis, Hoofnagle et al. (2019), provide a better approach. Their article is solely based on the new GDPR and the way it affects social life, private entities, and European integration. Contrary to the previously mentioned article, it is more structured around history, detailing the increasing dialogue of cyber matters, and how they were materialized – *e.g.* the 1995 Data Protection Directive as the premise of the GDPR [a fact that it is not mentioned by Markopoulou et al. (2019)]. Much like Christou (2018), Hoofnagle et al. (2019) focus on technical terminology and operation capability, with a particular emphasis on cyber governance and the challenges of cybercrime, even though the two articles distance themselves from the same point of leverage: while the former accentuates legal cooperation between the EU and European Union Agency for Law Enforcement Cooperation (EUROPOL) in relation to data-collection and information-sharing, the latter positions the GDPR's strategic implications as non-regularly for national security, complementing that criminal offenses are largely outside of EU-level competence.

This last part is particularly explained due to the hesitation that some Members States have, according to Hoofnagle et al. (2019), about letting such capacities to be handled by the EU. On the one hand, the GDPR does apply data processing by other governmental organizations and private entities that can or cannot operate in UE territory; on the other hand, it only permits governments to adopt special adaptations in their respective national legislations, which leads each country to update its national data protection regime (ibid.). Such conflict can intertwine with public interests, such as freedom of speech.

The polarizing magnetism of data protection is also a concern for Ruohonen et at. (2016), whose conceptions seem to be unlikely in a near future. It is important to notice how the article was published two years before the GDPR entered into force, but while it was still being regulated. The authors present an austere perspective due mainly to one of ENISA's primordial functions: an annually report made by national service providers about potential security incidents. This regulatory framework made CERTs notify ENISA at all costs and compose reports to also be sent do the European Commission (Ruohonen, et al., 2016). The system dealt with large amount of data and rapidly showcased an inconsistency in its composition, mainly because some Member States had under developing cybersecurity policies and capabilities, but also due to the idea that some national agencies were not able to prioritize technical solutions, leaving the reports to be unclear (ibid.).

Throughout this literature review, all authors agree that a major setback is the lack of common definition of cybersecurity – as well as other related "cyber-jargon" – in the EU's and the Member States' discourse, something which only accentuates the conceptual differences between prevalent actors and promotes barriers among them. The inequality between the MSs appears right away as an unavoidable issue: while it is still a present task that the Commission is trying to tackle, it remains as a measurement of interoperability mishaps, both aimed at national and international institutions.

Cavelty (2018) argues that cyber-power is multifaceted, in the sense that it can be used to shape the protection of web-usage, but also to create a malicious application. And that is exactly what the literature advocates that the EU should prioritize: the creation of a free and secure cyberspace, that works side by side with international partners and organizations.

1.4- The EU's impact on Member States in the field of Cybersecurity: the case of Portugal

The adaptability to new cybersecurity measures has been widely covered in this dissertation, mainly because of the efforts made by the EU and the respective responsibilities of each Member States. One of the examples of legal actions was to determine the capacity of the MSs to establish competent mechanisms of prevention and problem-solving techniques through CERT units. Each member had to establish national competent authorities composed of trained and specialized personnel. Portugal was no

exception and has been working as a pawn for EU's resilience to any type of cybercrime (Carvalho, et al., 2020; Christou, 2018).

While the technical and political integration in Portugal is being invested in, the academic debate is comparably far behind. This was the only topic whose scientific literature was not so abundant – something scholars believe will unavoidably change with time. However, we identified two articles that are able to provide an interesting and rich insight to the topic. According to Carvalho et al. (2020), Portugal has positively obliged to the EU's positions and initiatives, creating stronger legislation to fight cybercrime, and establishing common levels of network and information security.

Even though national governments, since 2013, developed a central part in preventing and responding to cyberthreats, Europeanization in small countries like Portugal usually works 'top-down' (ibid). From the Budapest Convention on Cybercrime in 2001, to the creation of the Portuguese National Cybersecurity Centre (CNCS) two years later, to the implementation of the GDPR, the authors defend that Portugal has been attentively following to the EU's guidelines, leaving room for future installations – specifically the School of Communications and Information Systems, that will serve as a centre for study and research in the cybersecurity area.

This level of hopefully enthusiasm is also shared by Silva (2019). Much like the previously mentioned authors, the creation of the CNCS is seen as a concrete evidence of efficiency and organization, dealing at the same time with "national management and coordination of response to cyber incidents, also ensuring international cooperation in this subject" (ibid.). Silva's work not only focuses on the definitions of cyber requirements and the indication of the legal framework: the author pinpoints, on a larger scale, Portugal's outcomes – 8th on the ranking of most vulnerable countries in the EU in relation to cybercrimes and top five on the percentage of cybercrime victims (ibid.:44).

The two scientific articles meet on what it is an uncertain and broad future for Portugal. While both compliment the country's determination in adopting a cybersecurity strategy, being eager to follow future integration and cooperating with fellow EU Member States, the bigger picture lies on the work that it still needs to be done. One the one hand, Carvalho et al. (2020) underline that some of the NIS Directive's obligations are not in full speed (although not mentioning which ones); on the other hand, Silva (2019) is keener on modernity, not only in updating national technological systems, but also on the way schools and hospitals, for example, can take advantage in knowing a little more about cybersecurity and all of its branches. The identification of security equipment and

requirements among the Member States was a way for the EU to take action while learning even more about the weight of cyberthreats. Portugal was not left behind, as it is still today involved in creating a larger field of action in all things cyber. However, as far as European Studies go, the topic of cybersecurity in the country is yet very undeveloped. By choosing to analyse the Europeanization of Portugal as a case study, our dissertation seeks to make a contribution to the wider academic debate on Europeanization of Cybersecurity and specifically on the Europeanization of Portugal.

Chapter 2- The EU's role in providing Cybersecurity framework:

> *"*We must develop capacities in trusted digital services and products, and in cyber technologies to enhance our resilience*"* (EU Global Strategy, 2016)

Cybersecurity has gained, since 2002, various degrees of relevancy. By the time ENISA was created, the EU was about to experience the largest expansion in terms of territory, population and number of Member States to date. Created by Regulation (EC) No 460/2004 of the European Parliament and of the Council of March 10th, 2004, ENISA's mission was primarily to enhance communication and cooperation between the EU's Member States, as well as to reassure a proper and secure framework for Network and Information Security (NIS) services. ENISA was – and still is – at the forefront of European Cybersecurity, facilitating and coordinating responses to cybersecurity incidents by elaborating support exercises with CERTs, raising awareness campaigns to the MSs (ENISA General Report, 2005), and gathering and analysing data on security incidents throughout the EU. The adoption of the aforementioned Regulation was a crucial step forward in the advancement of a "pan-European cyber" community – one that was later extended first by Regulation (EU) 526/2013, then invigorated by the NIS Directive (Markopoulou et al., 2019), and then fortified by Regulation (EU) 2019/881.

Progress in harmonization was one of the principal appeals of ENISA. As far as digital services are concerned, the Agency has issued reports to assist the MSs, especially when most of them did not have cybersecurity strategies properly tailored. Before ENISA, national and private entities worked in isolation and the cooperation with other countries happened not very often, which lead to divisive and rather confusing policies. To achieve an effective EU response, ENISA provided national protection intending to establish trusted communication guidelines and appropriate security measures (Markopoulou et al., 2019). ENISA has noted a qualitative understanding from Member States of threats, reinforcing the idea of a cybersecurity modelling formation (European Court of Auditors, 2019). As a result, ENISA has helped MSs to develop monitoring capacities for strategic analysis that will eventually strengthen a better and deeper understanding. Still, cybersecurity does not revolve mainly around digital threats nor online attacks that cover technological preoccupations; it affects social, political and economic matters, too (ibid.).

The sense of mutual support has always been seen as a pillar of the EU. In fact, in the initial Regulation, the Agency gave a prominent role to public authorities by "informing the general public, small and medium-sized enterprises, corporate companies, public

administrations, schools and universities" (EP and the Council, 2004: 3), prompting an information exchange between the Member States as a way of providing training, courses, and cross-border assistance. The objective is for ENISA to position itself as the centre of knowledge and expertise regarding cybersecurity procedures, creating a normative impact on the MSs (European Council, 2016).

The Agency also serves as the secretariat to the CERT Network – to encourage a rapid and effective operational cooperation between the Member States. However, the EU's goal to speak in unison constituted a major concern, mostly because not all Member States work at equal levels, and not all of them had established full-fledged response teams, given the fundamental disparities. But regarding cybersecurity strategies, there has been an increasing integration among the MSs. ENISA mapped the first inventory of 104 European CERTs, and made sure each one received the Awareness Raising Information Package (ENISA, 2005), as a way of promoting constantly updated practices.

For the first years, ENISA was successful in achieving levels of efficiency, and showed added value of acting at the EU-level. In their first annual report, from 2005, they registered three requests since starting operations – from the Communication Regulatory Authority of the Republic of Lithuania, in order to assist the implementation of their national CERT; to co-organize a training course in Vilnius to facilitate CERT training specialists across Europe; and, finally, to provide a technical opinion to the European Commission on the "Draft Assessment Report for the planned Communication on "Increased Security in Electronic Communication". ENISA accentuated relations with the industry, referring to it as an "important stakeholder" (ENISA, 2005). It also opened dialogue with NIS-representatives from non-EU States, such as Japan, Australia, Russia, and the US. During this period, close relations to international organizations were also constructed, particularly in the areas of network and information security. ENISA also worked with the Council of Europe to investigate possible synergies with foreign institutions, keeping cooperation and information exchanges on the table.

One of the key aspects of the formative years of ENISA was the establishment of the Working Group (WG) for risk assessment and risk management, that made up one of the main thematic areas addressed by the Agency's Technical Department. At the EU-level, it was constituted as a promise made by the Regulation to create "an inventory of existing methods" and "an information package for awareness" (ibid.: 32). By 2006, one of the deliverables of the first WG was the creation of a road map for future activities within ENISA that identify numerous tasks towards the enhancement of applicability of existing

risk management and risk assessment methods for various types of organizations (ENISA, 2006).

For the first two years of its existence, the Agency was standing on stable ground, creating relations with various organizations and painting an image of unity among the Union. But it was still an uncertain period, mainly because it was not until 2006 that its legal body was clarified and confirmed by the European Court of Justice (European Commission, 2006). By that time, it had already proved to be an essential bridge between governmental affairs and the private sector.

In 2007, ENISA still maintained a strong narrative of spreading awareness and institution-building among the Member States, while focusing on practical cases among local governments and Internet Services Providers (ISPs). The European Union contributed positively to the imperative importance of using metrics and key performance points as indicators for future analysis (ENISA, 2007). At this point, assistance was mainly targeted at the newly joined European States for better regulation and exchange of best practices. This was the case of Hungary and Bulgaria. ENISA supported the creation of cooperation initiatives between the two countries – as requested by the latter – as a way for the Hungarian experience to be transferred onto Bulgarian headquarters (ibid.).

The continuous support for national Computer Emergency Response Teams was something that was cemented throughout the years; this time, thanks to a more "hands-on" approach, ENISA encouraged the setting up of CERTs by preparing a series of presentation slides and lectures, as a way of ensuring the level of trust among European teams. This programme was used in a number of CERT projects in the EU and was a vital tool in the establishment of the Spanish government CERT.

EU CERTs got involved in what was known as one of the first large-scale cyberattacks within EU borders. Estonia, that relies heavily on its Internet infrastructures, was hit by a massive, politically driven Distributed Denial of Service attack (DDoS)[12] that oversaturated the websites of various banks and government bodies with unprecedented waves of spam and internet traffic. But as ENISA – and the European Union as a whole – argue, the country was fortunate enough to have a fully-formed CERT to coordinate the mitigation of those attacks.

[12] Distributed Denial of Services (DDoS) are attacks that make services or online resources unavailable by flooding them with more request and user participations than they can handle.

It is easy to understand that during this two-year period, the Agency was focused not only on major governmental enrolments, but on piercing immeasurably in the computers of home users and small and medium enterprises (SMEs) (ibid.). The critical point here comes down to the level of vulnerability and inexperience that categorized these users. According to ENISA (ibid.), they could have easily been victims of botnets,[13] have their data be used for obscure purposes, or be controlled by hackers. The European Commission shed a light on the role that public authorities played in keeping home users and SMEs properly informed about their own security. And on ENISA's 2007 report, it is highlighted that SMEs lacked suitable guidelines on implementing security and privacy apparatuses. Asked by the Commission, ENISA examined the "feasibility of European information, sharing and alert system, highlighting the Agency's role in fostering a culture of network and information security in Europe" (ibid.: 39) to conclude that almost 50% of the MSs did not have any information-sharing activity for Home-users and SMEs (ibid.).

However, it is important to notice that, on the contrary, the EU – and some Member States – has been paying attention to these gaps and has been producing mechanisms that help report risks and principal threats using NIS-influence practices to SMEs, since it is also promised on ENISA's future plans.

The role of ENISA was further strengthened because of the regulatory framework for electronic communications that was revised in 2009 that, in its genesis, implemented a reporting system of significant incidents to national regulatory agencies (Ruohonen et al., 2016). This section is more detailed in the State-of-the-Art chapter of this dissertation, but nonetheless it is important to point out how, to some scholars and policymakers, the existing system was exploited for institutional purposes, since it only covered internet and service providers, letting other private or public companies out of the picture (Burdon et al., 2012 in Ruohnen et al., 2016)[14].

Cybersecurity requires cooperation between public and private sectors, principally when it comes to shared information and to manage trust among involved actors. Poorly handled coordination can lead to system fragmentation, as well as a dispersal of expertise. The Council recognized the visible process that has been made throughout the years, but

[13] A network of computers infected with malicious software, controlled remotely by sending spam emails, steal information or launch specific cyberattacks.
[14] Burdon, M., Lane, B., & von Nessen, P. (2014). Data Breach Law in the EU and Australia – Where to Now? *Computer Law & Security Review*, 28(3), 296-307.

it still notices the level of untrustworthiness among some Member States (Council, 2017), hence, the launch of the Cybersecurity Strategy, along with cooperative structures outlined by the NIS Directive, aiming at a better, stronger, and more robust relationship among stakeholders. The assessment of such strategy has been placed on the Commission's working document entitled "Assessment of the EU 2013 Cybersecurity Strategy", where it consulted a number of stakeholders, varying from EU Agencies and bodies, to trade associations and industry representatives – including the European Cybersecurity Organization (ECSO) and the Alliance for the Internet of Things Innovation (AIOTI) – among others. The issue for stakeholders' consultation stated the following:

> "In order to identify the most appropriate mix of consultation methods, the first step has been to identify the relevant stakeholder groups and the best way to consult them in order to gather relevant input […] The Commission pays attention to differentiate data gatherings tools and adapts them to different types of contributions the stakeholders might have" (European Commission, 2007: 69)

However, this statement fell short of what ENISA had eventually evaluated. By taking a look at another Working Document on Impact Assessment by the Commission, the EU's approach to cybersecurity efficiency had not been sufficiently justified, subsequently in the lack of "synergies" between ENISA's activities and the interest of the stakeholders (European Commission, 2017: 68). Cooperation initiatives have been described as "immature" (ibid.: 23), paying special attention to a change in the culture of cybersecurity: one that does not necessarily go according to EU-level agreements. But to speak of the whole Union, it is important to acknowledge a lack in EU reliable data and analyses that have been covered for the past years. The same document detailed a larger concern for cybersecurity issues not being properly resolved in an equal manner among Member States – "such as the economics of cybersecurity, reliable trends of expected new challenges, the best solutions to face threats or criminal statistics related to cybercrime" (ibid.: 23).

The desire to improve cooperation is the rational belief behind ENISA's programme for 2019-2021. In fact, "cooperation" is one of the most frequently used words and it is materialized in the many collaborations the Agency participated in order to face future challenges. On the first pages, ENISA documents various activities that were shaped to prevent incidents in NIS-related challenges. The guidelines sought firstly to identify good practices by creating a more effective use of "secure software development life cycle

principles" (ENISA, 2019: 21). These initiatives had the assistance of the ENISA IoT SECurity Experts Group and the ENISA Industry 4.0 Cyber Security Experts Group (EICS). By the end of the same year, another partnership between ENISA and EUROPOL was launched in Athens, Greece – where the agency's headquarters is – with the main topic being the Internet of Things (IoT)[15] and how it can penetrate several day-to-day areas, such as transport, healthcare services, maritime security, and others. It is also significant to point out the memorandum signed in the previous year by ENISA, EUROPOL, EC3, and the European Defence Agency (EDA) that oversaw stouter developments in the field of cybersecurity by carrying out mandates in the areas of "exchange of information," "education and training," "cyber exercises," "technical cooperation," and "strategic and administrative matters" (ENISA, et al., 2018).

Many authors may question the steadiness of EU-level cooperation among its Member States – or even the transfer of competences (Wessel, 2019), but the EU's ambition in cyber matters can be formally regulated. By 2019, ENISA was working effortlessly in cooperation measures with the Member States, by either supporting incident-reporting activities, standardization of ICT security, assistance in capacity building, and even developing NCSSs. ENISA focused on innovation within the area, covering MS's approaches and initiatives with the help of official representatives from Spain, Austria, Poland, and the United Kingdom. The Agency offered direct support to individual Member States that requested the assessment and the improvement of their capacities in incident-response or technical training, including assistance in the preparatory phase of the Connecting Europe Facility (CEF) proposals (ENISA, 2019).

ENISA also produced an analysis of the EU's cyber skills development in the context of international activities and collected individual input from the Member States and their policies. These indicators contributed to the formulation of the Cybersecurity Skills Development in the EU (ENISA, 2019), that promoted education on cybersecurity matters among students of the EU, and the Cybersecurity Higher Education Database,[16] an interactive multimedia platform that provides cybersecurity knowledge and skills.

[15] Internet of Things (IoT) is a functional network between various electronic devices, software's and sensors that can communicate mutually and exchange data over an internet connection.

[16] enisa.europa.eu. *Cybersecurity Higher Education Database*. [online] Available at: https://www.enisa.europa.eu/topics/cybersecurity-education/education-map [Accessed: 10 Sep. 2020].

An issue that still remains unaddressed, maybe until the conclusion of this dissertation, is that ENISA is the only EU agency that has a fixed-term mandate with an expiration date for 2020; as pointed out by the Report from the Commission to the Parliament and the Council on the evaluation of ENISA, it limits its long-term functions to the Member States and EU Institutions, as well as to their stakeholders. The fixed-term mandate can also constrain the provisions of the NIS Directive, which entrusts ENISA with tasks with no end date (Markopoulou et al., 2019). Under the influence of the Proposal, the Agency would be granted a permanent mandate and be put on a much more secure and stable future (ibid.).

The NIS Directive is a legislative piece of coordination and management. While it defines with the Member States results and objectives in order for them to be achieved, it also leaves space for the MSs to choose the form and the means to do so. It was created as the first piece of EU-wide legislation on cybersecurity, and it entered into full force in August of 2016 (European Commission, 2020). According to article 4, the Directive mainly runs across two categories: operators of essential services (OESs) and digital services providers (DSPs) – and functions as an obligation to identify operators of key services in the sectors of energy, transport, healthcare, banking and financial market infrastructure, among others (EP and Council, 2016: 27, 29). By doing so, the Member States should provide information to the Commission on the application of such law provisions, having at the same time the responsibility of categorization and identification their own operators of essential services (Markopoulou et al., 2019; Wallis et al., 2020).

On article 5(2), it is explicitly lineated that the operator of key services must go in accordance with three criteria: “an entity [that] provides a service which is essential for the maintenance of critical societal and/or economic activities”, “the provision of that service depends on network and information systems”, and “incident[s] would have significant disruptive effects on the provision of that service” (Official Journal of the EU, 2016: 14). After an entity is considered to be on Annex II provided by the Directive of sectors and subsectors, the Member States must develop identification processes so that they can determine which individual company meets the additional criteria of operators of essential services (Markopoulou et al., 2019). By doing so, the Directive requests the MSs to adopt national measures to regulate these entities.

This was a crucial point in EU regulatory methods to be incorporated by national authorities. For the first time, each Member State was responsible to designate one or more Computer Security Incident Response Team (CSIRTs), fortifying the cooperation

between the MSs and the European Union and to establishing a multilateral information exchange. Through article 12(2), a CSIRT Network, largely made of national CSIRTs and EU CSIRTs, was composed and was, therefore, responsible for risk and incident handling – these teams need to first fulfil the requirements listed in Annex I of the Directive, as it points out adequate resources and appropriate equipment for CSIRTs (Official Journal of the European Union, 2016).

However, the Directive does not impose a hierarchy for the competent authorities; they need to be regulated according to the single characteristics of their own national bodies. What matters is that, as a whole, they need to achieve with the objectives provided by the EU, and in by doing it, the MSs had to come up with a structure that suited them. Article 10(1), states that:

> "Where they are separate, the competent authority, the single point of contact and the CSIRT of the same Member State shall cooperate with regard to the fulfilment of the obligations laid down in this Directive" (Official Journal of the European Union, 2016: 17)".

While article 12 is responsible for creating and establishing a network of national CSIRTs, the Commission participates as an observer, and ENISA provides secretariat services, as well as actively supporting the cooperation among CSIRTs. Every 18 months after being active, every CSIRST network has to produce a report assessing the benefits of operational cooperation, including their own conclusions and recommendations. Afterwards, these reports shall be sent to the Commission as a contribution to the review of the functioning of the Directive.

In order to safeguard that possible changes in the market are truthfully reflected, Member States need to, at least every two years, update their lists of identified operators of essential services, as well as adopting legislation to ensure a higher level of security, like it is sustained in Article 3 of the Directive. Even though it creates a more transparent approach to security procedures, the issue of cooperative relations between commercial entities, for example, can come across as difficult to verify, since commercial organizations are generally reluctant to disclose any incidents – fearing a toll of negative impact on company value (Aleksandrowicz, 2020). Still, the Member States have the responsibility to ensure such forms of cooperation and trust among the many sectors by creating a culture of reporting situations of their corresponding security networks, information and communication systems (ibid.).

In correspondence, digital service providers consist of every legal person that provides a digital service, paying special attention to the online marketplace, online search engines and cloud computing services – as they are described on Annex III of the Directive (2016). Their regulation is built upon the fact that multiple businesses and companies depend on these providers for the provision of their own services. Unlike the operators of essential services, it is important to note that the NIS Directive does not request digital service providers identification by the Member States (EP and the Council, 2016), warranting a catch-all approach. Still, the Directive, in Article 16, points out security measures that digital service providers should take in consideration when endorsing a level of security for network and information systems (ibid.: 21, 22). DSPs, in fact, are required to take appropriate security measures and to notify them to competent authority figures (European Commission, 2018).

Being the Directive a public-access document, it gained greater relevance for being the first of its kind to showcase how the EU tackled NIS-related issues at such a high level. In October of 2019, three years later after its implementation, the European Commission published an overview report (European Commission, 2019) that displayed how the Member States have behaved during this time frame and also how they were able to identify operators of essential services who have to put in place cybersecurity measures and report them due to their relevancy and a major influence in security-related planning.

In the report, it is clear to see that the Member States relied heavily on prior experience with OESs, varying their type of methodology according to national provisions, as well as with the Council Directive 2008/114/EC on critical infrastructures. However, in most cases, the identification process follows a top-down approach, conducted by public authorities (European Commission, 2019). The number of identified services by the countries, as noted by the Directive, has an average of 35 services per Member State (ibid.), with the total number fluctuating from 12 to 87, as shown in Annex 1 of this dissertation. The study (ibid.) also shows that the density of each Member State does not dictate their capacity in indicating more services – as it is to be expected since "practice consumer and companies usually have access to the same types of services in all Member States, irrespective of a country's size" (ibid.: 10). In addition, the study also highlights different interpretations by the Member States as to what constitutes an essential service under the NIS Directive. This ambiguous conclusion makes it difficult to compare lists of existing essential services and puts at risk the scope of the Directive,

as some operators are being exposed to additional regulation, while others, providing similar facilities, remain omitted (ibid.).

Overall, while the NIS Directive broke ground to enhance and improve risk management habits among the European Union, the Commission still advises the Members to be as consistent as possible, making full use of guidance documents developed by the Cooperation Group – under the Commission's aegis – to further align the list of essential services and the qualitative or quantitative thresholds used to identify OESs. Member States should also work alongside to strengthen a cross-border operation cooperation systems.

The NIS Directive works complementarily with the General Data Protection Regulation. While both law-making processes do not mention each other in their texts – the Directive only briefly touches on data protection in its article 2 –, it is clear how the two accompany each other in their aims to secure data protection and reinforce cybersecurity strategies. When it comes to personal data, while the first works with a broader and expansive system, providing the Union high level of NISs in order to improve the functioning of the internet market, the second one specifies in programmes of personal data security and free movements of personal data (European Court of Auditors, 2019). And while the Directive established a national strategic plan for the Member States to designate competent authorities, the GDPR traces rights to "data subjects", "obligations to data controllers" and "rules for transferring personal data" (ibid.: 15).

The GDPR became applicable in May 2018 and for the first time saw the EU form more careful planning on personal data. It can be described as a more structured and sturdier adaptation of the 1995 Data Protection, in a way that filled the gaps in national privacy laws and transparency within countries of the European Union (Hoofnagle et al., 2019). Now, the GDPR is dealt with court-wise, "combined with persuasive, albeit non-binding, interpretation by the newly created European Data Protection Board" (ibid.: 71).

The GDPR works largely with big data and machine learning business models. However, it starts by defining its main scope to the protection of identifiable natural persons (EP and Council of the EU, 2016: 32), that goes beyond personal name or addresses: public or non-sensitive information, IP addresses, cookies, pseudonyms, and similar data, all fall under this type of categorization, showing a much broader sense of modern personal data. Every time any corporation processes personal data – whether it is by collecting, destroying, organizing, storing it – the Regulation is put to test (EP and Council, 2016: 33). The actors involved in processing information, being that public or

private, are recognised as "controllers" (ibid.), mainly companies; the ones who determine the purposes and the means of processing personal data are named "processors" (ibid.), those that effectively do something with one's data, such as cloud providers or data centres. The GDPR requires that controllers make sure that processors are competent and responsible, forming a "chain of accountability" (Hoofnagle et al.: 73), as a way for processors to be blocked from delegating operations without the permission of the controllers. For companies, for example, regulatory processes become more overcontrolled inside territorial legislation. The GDPR imposes controls on personal data outside the EU, protecting data for EU-citizens that are handled by non-EU organizations or outside EU borders (EP and Council, 2016).

Consent is one of the most substantial parts of the Regulation. In article 7, the GDPR states that consent must be exclusively informed, and up to the responsibility of the data subject, as a way of which the withdrawal must be as transparent as the authorization of consent itself (EP and Council of the EU, 2016). While the Regulation has stringent requirements and forbids burying consent in miscellaneous and uncharted forms of presentation, it still recognizes contractual procedures as a necessary basis for legal contracts (Hoofnagle et al., 2019). Companies can store IP addresses from users during brief periods of time for reasons of security or scam prevention –by doing so, they are not going against the Regulation, if such decisions are publicly announced and directly targeted to users.

The GDPR once again prioritizes users' free-will at providing treatment of personal data. Special data processing is another part of the agreement. It is defined as information that disclosures opinions, political positions, religious or philosophical inclinations, sexual orientation, ethnic origin, biometric data, among others (EP and Council, 2016: 38). Legal processing of sensitive data is forbidden by the GDPR, even though there are some exceptions. In some categories, consent is again at the forefront of the discussion, dictating strong measures to be taken by the Member States, where the law "provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject" (ibid.).

Besides unique users, the GDPR states new provisions to the Member States, as they must notify the Commission, assuming the form of a supervisory authority, on matters such as data protection authorities and national law incorporation of the Regulation – in addition, the reports to the superlative functioning bodies of the GDPR must come as a way to protect the fundamental rights of natural persons (EP and Council of the EU, 2016: 65). It is up to the Member States to lay down penalties related to other applicable

sanctions in case of violation of the Regulation, too. The penalties in question must be "effective, proportionate and dissuasive" (EP and Council of the EU, 2016: 83). It is also the responsibility of the MSs to process personal data in terms of employment situations, protecting personal interests of the workers, by transferring data to a responsible group of the respective enterprises that engage in monitoring it, or by transparency in employment contracts, regarding the safety, equality and diversity in work environments. Whether it be in the workplace, public spaces or private life, the right to secrecy must be encouraged by the Member States as a way for controllers or processors to create a necessary and proportionate right of personal data with the obligation of secrecy (EP and Council of the EU, 2016).

In the context of propelling union discourse between the MS, article 97 subsequently has a relevant nature in status reports with the objective to analyse the present regulation of the GDPR. Every four years, the Commission presents to the European Parliament and the Council what each country detected regarding their continuous review and evaluation of the Regulation. At a minimum requirement, the reports need to circumvent Article 5 on the transfer of personal data to third countries or international organizations and Article 7, that refers to cooperation and consistency mechanisms. What ends up being such a critical process is the fact that the Commission can "submit appropriate proposals to amend this Regulation" (EP and Council of the EU, 2016: 87). The Member States have prepared for their first review of the application of the GDPR, whose deadline ended on May 25th, 2020.

A general note from the General Secretariat of the Council to the national Delegation, issued in October of 2019, features comments from 19 MSs, focusing on areas where they observed conflict, and questions about clarity and recommendations for future problem-solving. For example, in Germany, some businesses and governmental agencies have felt overwhelmed by the GDPR's entry into application, with some users feeling some level of uncertainty with the new digital panorama it created (General Secretariat of the Council, 2019). Nevertheless, the country showed a consistently positive approach of encouraging and recommending an undeviating and uncomplicated application of the GDPR, by working closely with data protection agencies and authorities. Still on this idea of unification comes the remarks of the Czech Republic that points a finger at some of the policies of data protection among the Member States. The country affirms that before the creation of a universal sense of unification, there should be greater national ownership of the GDPR, in order to stimulate domestic debate on such topics such as the online age

of consent. Yet, the Regulation tens to trail the political specificities of each national culture rather than the logic of businesses, which influences which rules to apply to each country.

About the effectiveness of the EU supervisory authorities, the Member States made comments about expectations on cooperation. Latvia and Lithuania are used as examples to justify such a case. Both in terms of examining a specific mishap, or when enforcing the correction of obsolete measures, several complaints have been successfully rectified by cooperation between the two countries and their corresponding supervisory authorities. Through these meetings, several apparatuses were created to ensure a consistent approach in collaboration within member, as well as with the European Data Protection Board (EDPB).

Lithuania, in response to the GDPR, created two supervisory authorities – the State Data Protection Inspectorate, that deals with human, technical and financial resources, and the Inspector of Journalist Ethics, that stores data for journalistic, academic and cultural purposes (General Secretariat of the Council, 2019: 35). However, it also made some remarks on some provisions of the Regulation, especially in the areas regarding processors, in which recommends the alteration of the information stated in the preamble 81, as a way of not causing any lawful uncertainty; and the right of access by the data subject, in which Lithuanian data controllers have doubts about the period for which data subjects must be accustomed to access certain personal data, and about the existing restrictions to obtain a copy of it.

Concerning the application of the GDPR, most countries found purposeful ways to integrate its provisions in national legal authorities, with particular interpretations that make this legislation anything but steady. In June of 2020, the Commission prepared the first evaluation review of the Regulation, saying that it efficaciously met its objectives, mainly those of strengthening personal data protection, keeping the free flow of personal data within the EU, and spreading awareness to the European population on its content. The same document affirms that nearly 71% of EU citizens "know about their national data protection authority […] the rights of access, rectification, erasure and portability of their personal data, the right to object to a processing, as well as enhanced transparency" (European Commission, 2020: 9). Regarding data subject rights, the report refers to a clear, but still unused potential, to "put individuals at the centre of the data economy" by allowing to freely change between services providers, to combine various services, and to choose the most data protection-friendly ones (ibid.: 8). In contrast, the Commission

notices that a development for future European data protection cooperation is still in the works, and that a documentation of cross-border situations deserve an adequate form of action. It also acknowledges a future discrepancy among data protection authorities in the Member States, creating bifurcated paths between countries that are more technologically savant and countries whose technological power is not as consistent.

Cybersecurity strategies can be seen as a continuation of the internal and external policies that have been developed by the EU in the areas of former legislation processes, like the NIS Directive. The EU is still to this day a prominent actor in developing and executing legislation to all dimensions of cybersecurity. The topic has not lost any relevancy in these past years, remaining high on the European agenda. The last example came into fruition after an agreement between the Council on December 2018 (European Commission, 2018) to adopt new cyber-resilience packages to reinforce the deterrence and defence of the Union. The text was later proposed to the European Parliament in March 2019, followed by the Council a month later. Shortly after, the newly formed Cybersecurity Act became active on June 2019. To underpin the proposal and collect evidence, the Commission ran two public and dedicated objectives that were laid down as the premise of the Cybersecurity Act: the reform of ENISA and the creation of a European cybersecurity certification framework.

ENISA resurges again, but this time the eagerness to reinforce its actions starts with the implementation of a permanent mandate, in order to improve and achieve more effective results. The Agency was given a new interactive power in areas such as operational cooperation and ICT security certification, along with a solider grip of assisting the Member States in developing their CSIRTs (EP and Council, 2019). The MSs will now receive not only technical advises on how to improve their capabilities to detect and respond to incidents, but ENISA will also analyse national vulnerabilities based on available information.

To maintain cooperation at the EU level, ENISA was entrusted with the task of supporting both the MSs and the Commission by implementing and regularly reviewing the existing general cybersecurity policy and the key strategic sectors identified by the NIS Directive, such as finance, transport, energy and so on. On preamble 15, on the first pages of the Act, the importance of this role gives at the same time a platform to previous work made by the Union to ensure security in digital technologies. Thereby, ENISA became the “technological hub” (ibid., 2019: 17) for the Member States: a functioning institution for cybersecurity information from EU institutions and bodies

ENISA also grew in monetary funds and recruitment in human resources. Every financial year, the Executive Director must draw up a draft statement of the Agency's estimates revenue and the following shall proceed to the Management Board. The latter, based on the findings of the former, shall then produce a final version of the document concerning ENISA's revenue and expenditure (EP and Council of the EU, 2019). The European Parliament will afterwards accept the established plan. The Union's budget will be crucial if necessary, adjustments to ENISA's budget and programming document should happen, as it becomes final after the definitive adoption of the general budget for the EU. Provided by the European Commission, the initial budget for the year 2017 was 11.2€ million, predicting a steady increase over the years. It is expected to reach in a near-future an estimate of 23€ million, with a growing number of employees as well (EP, 2019).

To cover the second task of the Cybersecurity Act, it is central to understand that European cybersecurity certification schemes are envisioned to create a better sense of harmonization and security within the Union, contributing also to increase the level of cybersecurity practices and initiatives among Member States (EP and Council, 2019). The certification framework was approved by the Commission and then required by interested companies for their ICT products, ICT services and ICT processes. Recourse to the cybersecurity certification remain voluntarily, except when confronted with ingoing law by the EU (European Commission, 2020). According to the Act, it is appropriate to link the responsibility of these certification schemes to manufactures of ICTs; however, Member States should not be prevented from adopting, or even creating, national cybersecurity certification framework for national security purposes. They can also be in contact with the Commission and the European Consumer Consultative Group (ECCG) for any kind of delineating new certification schemes. The last two will then evaluate the potential of these new proposals and estimate their functionality on internal markets.

Chapter 3- Analysis: The development of cybersecurity framework in Portugal

3.1- The formative years: from the creation of the Green Book to the first CERT unit

The debate on cybersecurity emerged within the Portuguese landscape at an unhurried and irregulate pace. In the late 1980s and 1990s, national policy makers mirrored what the EC/EU was passing on and talking about – opening dialogue for the first time in 1989 through Recommendation No. R (89)9, that fixated not specifically in cybersecurity policies, but on the resurgences of cybercrime in a European context. The document ensured such tasks to the MSs from the implementation of good practices to principles regarding circulation of information on data protection on the employment sector (European Council, 1989).

In Portugal, while the country joined the EC in 1986, conversations on this matter started gaining form in the 1990s – in a time where cyber issues were not so socially prevalent and urgent. However, in order to meet EU-level criteria, the Resolution of the Council of Ministers no. 16/1996 was published, establishing a Mission Team for Information Society that would eventually support the national Ministry of Science and Technology to create the Green Book for Information Society, introducing cybersecurity methods to the political agenda (The Resolution of the Council of Ministers, no. 115/98). The Green Book, formally introduced in 1997, was the first political document that took into consideration the protection and integrity of computerized data, while simultaneously promoting a free and accessible use of websites to companies, schools and private citizens. It came from a process of diffusion of European political guidelines, notwithstanding a market-targeted nature, made to increase users' safety in online commerce by implementing important software solutions into a broader, european – and even global – market.

In 1998, shortly after, the National Initiative for Electronic Commerce was created as a way of enforcing appropriate tools for the fast growing of Internet usage in Portugal. And while it commended the creation of a unique currency among European borders to further strengthen inter-territory trades and partnerships – it felt mandatory to first define a legislative body of work that provided conditions to expand online commerce with the creation of an "applicable juridical regime for electronic documents, as well as digital

signature and electronic invoice" (The Resolution of the Council of Ministers, no. 115/98: 4542).

Portugal was thus involved in creating new cybersecurity capacities that could meet international and institutional objectives. The EU had been stimulating the MSs to take present challenges within the cyber world into consideration and asked them to respond accordingly. By doing so, it encouraged the creation of awareness campaigns, the setup of a stronger dialogue with international organizations and partners of NIS operational systems, as well as an investment of network and informational security solutions – not only in telecommunications and data protection, but in providing a defence in anti-virus software (Commission of the European Communities, 2001). However, it also implied responsibilities to the MSs, especially in reinforcing their CERTs, and working on improving the coordination among them. The process of Europeanization was ongoing and showcased how the EU was able to connect its national and european teams alongside ENISA. The Commission asked the Agency to develop trustworthy relations with the MSs and the corresponding stakeholders to develop an appropriate data collection framework (EP and the Council, 2017), but also to improve the European capability to respond to network security threats (ibid).

However, by the early 2000s, Portugal, in contrast with other European countries, still did not have a composed computer response team. In order to tackle growing cybersecurity incidents, the Foundation for National Scientific Computing[17] trained several employees to establish such goal and thus created the first CERT unit, in 2002, to provide services under the National Research and Education Network[18] (Santos, 2014). CERT.pt functioned at the national level, providing at the same time assistance and coordination to other correspondent european CERT entities; it was also accountable of producing reports on recent incidents and promoting a secure culture among public and private spheres of influence. Throughout the elaboration of this dissertation, CERT.pt remains the only national governmental CERT to be a certificate candidate by the Trusted Introducer for CSIRT in Europe, having received its accreditation in December 2015[19].

Portuguese participation in the cyberworld was still a bit far behind in comparison with other MSs. By 2005, Portugal and Cyprus were still the only countries without a

[17] In Portuguese described as the Fundação para a Computação Científica Nacional (FCCN)
[18] In Portuguese described as the Rede Ciência, Tecnologia e Sociedade (RCTS)
[19] CERT.pt could be the 20th certified european CERT by the Trusted Introducer for CSIRT in Europe: https://www.trusted-introducer.org/directory/country_certification_Z.html

National Liaison Office to further the communication between the members – such competences swayed between Pedro Manuel Barbosa Veiga, president of the FCCN, and Manuel Filipe Pedrosa de Barros, director of the National Authority of Communications[20] (ENISA, 2005) –, a position that would only be filled in in 2007.

3.2- The Budapest Convention

One of the first European efforts that translated into national legislation came after The Budapest Convention of November 2001. The Convention, organized by the Council, served as an example of one of the first global efforts regarding cybersecurity discourse, recognizing cybercrime as a borderless issue; through the use of substantial criminal rules, procedures and international cooperation, the main goal was set to harmonize the various laws of the MSs, thus promoting a more effective principle in achieving better policies. Serving as a key-figure for a European legislative common-ground, the Convention saw the countries delegate responsible authorities, enunciate declarations and design territorial applications (European Council, 2001).

Portuguese participation was crucial in terms of national policy and European recognition. It resulted in the designation of the Judiciary Police[21] as a constant contact point for computer systems or data related issues – as rectified in Article 24[22]. Increased Portuguese participation also included the transition of new legislation into Portuguese law, which entered into force by Law 109/2009 (eight years after the Convention took place), showing a path that would lead to the Cybercrime Act. According to the ruling by the Lisbon Court of Appeal, this new legislation outdated the Computer Crime Law of 1991 and its fallacies, especially when it came to protecting and accessing traffic data[23], as they became more manageable by a competent national judicial authority. The Cybercrime Act also introduced a procedural regime applicable not only to cases related to crimes provided in the respective law. Article 11 includes cases related to crimes committed through a computer system or in any case in which it is necessary to apply any

[20] In Portuguese described as Autoridade Nacional das Comunicações (ANACOM).
[21] Reservations and Declarations for Treaty No. 185 – Convention on Cybercrime: https://bit.ly/2ZI8K3u
[22] Article 24 of the Convention of Budapest refers that each Member State shall designate a point of contact available twenty-four hours a day to ensure immediate assistance in the field of investigation, or proceedings concerning criminal offences within cyber-related incidents.
[23] According to article 2 of the Cybercrime Act, Traffic Data refers to computer data related to a communication process made by a particular system, in which it is indicated the origin of the communication, the destination, the route, the time, size, duration and the service.

electronic support (Portuguese Official Journal, 2009 & The Lisbon Court of Appeal, 2013). It is important to also highlight how the Cybercrime Act in Portugal enabled international relations in order to fight crimes related to informational systems. Article 21 builds a bridge between national and international authorities by creating several European contact points that have access to similar and updated information, facilitating permanent assistance and discourse; particularly in areas that touch on "technical advisement to other contact points", "explicitly preservation of data in emergency situations or delay", "the collection of evidence for competent purposes in cases of emergency or delay", and, also relevant, "the location of suspects and the provision of legal information in cases of emergency or delay" (Portuguese Official Journal, 2009: 6323).

3.3- The formulation and creation of the Portuguese National Cybersecurity Centre

Portugal was subject to several kinds of pressure in establishing a physical body of work dedicated to cyber-matters. Some MSs already built their own versions a few years prior – as Ireland did in 2011[24] and France in 2009[25]. Through Resolution of the Council of Ministers no. 12/2012, Portugal consolidated and implemented the National Information Security Strategy. This Resolution sought to approve a plan of action to reduce the cost of ICTs in Public Administration, but also to construct an operative "information systems architecture, which will serve as a guide in the implementation, acquisition, development and maintenance of information technologies and systems in Public Administration" (Portuguese Official Journal, 2012: 598). It first predicted a deadline of six months to implement in ICT-related contexts new "architectural proposals of integration references and norms" and then a projection for twelve months in implementing "ICT cataloguing tools, methodology and definition of security and sectoral standards and guidelines" (ibid.).

In this document, we notice the lack of normative data in order to sustain the implementation of such Regulation and the responsible actors. There is no definition of a

[24] The National Cyber Security Centre (NSCS) encompasses the State's National/Governmental Computer Security Incident Response Team (CSIRT-IE): https://www.ncsc.gov.ie/
[25] The National Cybersecurity Agency of France (ANSSI) works as the national authority for cyberdefence and network and information security (NIS): https://www.ssi.gouv.fr/en/cybersecurity-in-france/the-national-cybersecurity-agency-of-france/

budget, nor clearly measurable objectives, as well as the political instruments determined to achieve such ends. However, its mission remains vital because it presented, for the first time, the Installation Commission of the National Cybersecurity Centre that was later assigned to the National Security Office (GNS) by Resolution of the Council of Ministers no. 42/2012.

This Commission would define the proper methods and instruments for the "creation, installation and operationalization" (ibid.) of the National Cybersecurity Centre, and would be composed by various representatives of cybersecurity in Portugal – conjugating members from Homeland Security, the Ministry of Internal Administration, and the Ministry of Justice -, as well as other people nominated by the Prime-Minister, to whom it was presented a final report on June 30th, 2012, when all functions would cease (Santos, 2014; Portuguese Official Journal, 2012).

ENISA had previously detailed the creation of a national strategy for cybersecurity to be a common aspect between all MSs; one that still required special attention to certain tasks: to potentialize the development of national CERT communities; to involve national interest groups as a way of incorporating the interest of different stakeholders; to promote political involvement among ministries with security and crisis management responsibilities in developing newer strategies; to include civil society in awareness and support exercises, to involve owners of critical infrastructure; to assign the Government as a facilitator in order to operate in such activities like information-sharing and international cooperation; among others (ENISA, 2012). Portugal worked in accordance with these requirements and, in 2013, the Government launched a review of the Strategic Concept of National Defence, thanks to Resolution of the Council of Ministers no. 19/2013 – that takes into account "the need to protect the functioning of the economy and society from cyberterrorism and cybercrime" (Carvalho, et al., 2020: 6). Among the priorities, the document stood out for granting the protection of informational infrastructures with the creation of the National Information Infrastructure Protection System[26], creating space for the establishment of a functioning structure in control of cybersecurity procedures, by paying closer attention to systems' vulnerabilities and encouraging the intervention of civil-military capacities (Portuguese Official Journal, 2013).

[26] In Portuguese described as the Sistema de Proteção da Infraestrutura de Informação Nacional (SPIIN).

A few months after, presented as a way of granting protection and resilience to information networks and ICTs, while ensuring the country's determination as a necessary actor in the cyberspace regarding national interest, Order no. 13692/2013 cemented the guidelines later used to establish cyberdefence, determining the position of the National Cybersecurity Centre at the dependence of the General Staff of the Armed Forces (Portuguese Official Journal, 2013; Ministry of Economy, 2018).

The same document was presented as an Orientation form for Cyberdefence policy and embedded the military practices that were mentioned above. In its guidelines, it is important to detail a revision of the Basic Law of the Armed Forces Organization as a way of laying down "a structure of command and control of national cyberdefence" (Portuguese Official Journal, 2013: 31978) by contemplating a body of work with strategic-military orientation that could operatively respond to cyberthreats and incidents (ibid.), as well as the construction of an open-ended dialogue with similar international forces – mainly others working CSIRTs – with the objective of sharing information, promoting synergies, and reporting active malicious activities.

To an extent, Portugal was adjusting to a risk-reducing, technological-concerning regulation at a slow pace, namely compared to the short-term goals already envisaged by the EE.

Also, in 2013, the Union passed the "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace". With this new policy, the Commission distributed different roles to the several institutional bodies working on cyber resilience, as well as new responsibilities to the MSs. The Strategy did not require ENISA to do anything particularly new, but to continue its efforts in carrying out "strong national cyber resilience capabilities" (The Commission, 2013: 7) and to support the MSs and other EU institutions in achieving a pan-European scenario regarding cybersecurity exercises – such as the "Network and Information Security driving licence[27] (ibid.). The Strategy required EUROPOL, and more precisely the EC3, to provide analytical support to the Member States' cybercrime investigations, not forgetting the production of reports illustrating emerging threats and trends in the cyberworld.

Regarding the Member States, despite recognizing growing consciousness on the topic, the Commission advised the latter to designate national competent authorities for NIS, as well as a national NIS strategy and a national NIS cooperation plan, so that it

[27] The "Network and Information Security driving licence" was proposed in 2013 as a voluntary certification programme to enhance technical skills and competences among IT professionals.

could finally solve the fact that not all EU members have an operational capability response to effectively tackle cybercrime. The Commission also invited the countries to make good usage of the purchasing power of public administration by stimulating the improvement of ICT products and services and promoting an early involvement of Academia and the Industry sector's attention on the research agendas of civilians and military organizations (The Commission, 2013).

The document did not have the desired effect it sought out to have in Portugal automatically: by this time, the country was still far behind on the deadline set out by the Commission for the construction of a national and physical CERT. In 2010, the Commission set out 2012 to be the definite deadline for MSs to construct an emergency response team that works in efficient and in secure conditions, as well as consequently the creation of a network of these national emergency response teams to operate at an EU-level (The Commission, 2010).

It was only on May 9th, 2014, that the creation of such an organism was approved with Decree-Law no. 69/2014 that defined the terms of the National Cybersecurity Centre, which still operated within the guidelines and the orientation of the GNS. The assignment in question was clear:

> "Within the scope of the GNS, the National Cybersecurity Centre, hereinafter referred to as CNCSeg, whose mission is to help the country in a free, reliable and safe way, by promoting the continuous improvement of national cybersecurity and international cooperation, in articulation with all the competent authorities, as well as the implementation of measurements and instruments necessary for the anticipation, detection, reaction and recovery of situations that, in view of the imminence or occurrence of incidents or cyberattacks, jeopardize the functioning of critical infrastructures and national interests" (Portuguese Official Journal, 2014: 2713).

The CNCS started working on October of 2014 and presented itself as a mechanism to assure the security of the State's ICT systems as well as the country's most critical infrastructures, while promoting cooperation between all cybersecurity actors. With the Resolution of the Council of Ministers no. 36/2015, the Centre was defined as a national authority on issues related to the cybersecurity, functioning primarily on six strategic axes: 1) structuring safety within the cyberspace, that required a stronger and transverse leadership based on establishing a political-strategic coordination alongside the Prime-Minister; 2) combating cybercrimes, by certifying a constant update of the present legislation in order to perform at maximum efficiency; 3) protecting the cyberspace and its working infrastructures with improvements of information systems that affect public

and private entities and its citizens; 4) educating, preventing and raising awareness among all users of the internet; 5) investing in research and technical development to achieve national solutions; 6) lastly, fomenting cooperation among national and international partners (Portuguese Official Journal, 2015: 3738).

Consequently – and taking into account the previous lines –, on the official website, the Centre provides a consistent and coordinated response to incidents, articulating between producing mitigation recommendations and screening incident reports and their technical and forensic analysis. In March of 2015, the CNCS expanded its functioning capacities by adopting the CERT.pt's responsibilities thanks to an agreement made with the Foundation for Science and Technology (FCT)[28].

To respond to axe 1 of the Resolution of the Council of Ministers no. 36/2015, the Centre is a member of the National CSIRT Network, sharing the common goal of establishing bonds of trust in computer security areas. With a total of 31 full members, the Network is constituted – in addition of the CNCS – by public administration, communication and banking entities, the energy sector, the Armed Forces, Universities, internet service providers, among others[29]. It is with these organisms that the Centre works with in order to establish a national response to incidents: by speaking within a similar nomenclature in order to share vital information among themselves (Portuguese Official Journal, 2015).

3.4- International cooperation with other MSs and reporting to ENISA

There is also active cooperation outside Portuguese borders that touches the cornerstones of information security and go accordingly with European objectives as well. According to a source at the CNCS (I1), one of the most important aspects for European resilience in terms of cybersecurity is based on models of trust and information sharing: active cooperation with other MSs in the light of European legislation plays an important role "in coordinating actions aimed at anticipating and mitigating threats within the cyberspace" (I1). In fact, it is mentioned on article 12 of the NIS Directive the willingness to share information and build better preparedness through and improvement of

[28] In Portuguese described as the Fundação para a Ciência e a Tecnologia (FCT). In 2013, the FCCN, which had the status of a private Portuguese non-profit institution of public benefit, was extinguished and its competences were transferred to the FCT.
[29] National CSIRT Network, *Rede Nacional de CSIRT*, [online]. Available at: https://www.redecsirt.pt/ (Accessed: 18th September, 2020).

situational knowledge *à priori* and during the course of cybersecurity incidents that affect the MSs (EP and Council of the EU, 2016). However, apart from responding to incidents, there are also different ways of establishing cooperation with european CSIRTs. I1 refers the formulation of joint projects, exercises and training workshops that promote "continuous evolution of various National CSIRTs, in order for the most advanced ones help the evolution of the others", thus building a higher level of maturity when responding to threats. One example is Portugal's participation, especially during the transpositional period of the NIS Directive, in European WGs, that were created with the objective of providing assistance to the MSs – as the Centre served as the only single point of contact designated (European Commission, 2018). Even though there are not many instructions made by the Portuguese delegates to the WGs, priorities tend to change across time, as a result of MB's participation in those meetings.

While maintaining a European-level approach, the competences of EU agencies – in this particular case ENISA – are seen as guidelines that serve as benchmarks for the implementation of European policies later adopted by the MSs. In effect, Regulation 2019/881 points out such description of ENISA. In article 4, it emphases the agency as a "centre of expertise on cybersecurity" […] that "shall assist the Union institutions, bodies, offices and agencies, as well as Member States" (EP and Council of the EU, 2019: 35), promote cooperation, increase the MS's cybersecurity capabilities; but also support national and Union CSIRTs in promoting dialogue and ensuring each one possesses a common set of proficiencies and works according to best practices (ibid.). I1 refers to the EU's acting as a pivot in its cooperation alongside EU institutions and the MSs. Portugal, in this sense – and like it was previously mentioned – operates in open dialogues with ENISA at a frequent rate: according to the CNSC, not only it participates in ENISA's management composition, by being a part of the National Liaison Officers Network[30], but is also a member of some of the WGs it creates (ENISA, 2019). Therefore, the tasks and responsibilities of ENISA (but also, significantly important, of the CNSC) result in multiple interactions, in which "the regularity or frequency is determined by the subject in question" (I1).

Nationally speaking, so far, most of the legislative processes implemented in lawful territory circled around the same bullet points – cooperating with similar national and

[30] The National Liaison Officers Network works as an important organ of ENISA that facilitates the exchange of information between the Agency and the Member States, providing at the same time relevant recommendations to stakeholders across the Union.

international organizations, raising awareness at various levels and administering a stronger defence force when tackling cyberthreats. At this time, the country was able to accompany with the recent orientations made by the EU – knowing still that the creation of the Centre came with a two-year long delay –, and there was an evolution of national positions that reflected Portuguese interests (CNSC). However, by going back to the NIS Directive, it is comprehensible to conclude that it was a major transformation, not only for Portugal's position in the European framework, but also for its core structure of internal security - providing functioning data bases for any private or public working entity so that minimum security requirements for NIS can be easily achieved and have less constraints (I1).

3.5- The transposition of the NIS Directive

The transposition of the NIS Directive occurred in August 2018 and was led by the Presidency of the Council of Ministers and the CNCS, under the wing of the National Security Office. Through the Law no. 46/2018, it explicitly mentioned the adoption of security and incident reporting requirements for critical infrastructure operators, for essential service operators, as well as for digital service providers. Likewise, for the CNCS, it meant a reinforcement of its roles as a National Cybersecurity Authority and also saw its functions of regulating, supervising inspecting and sanctioning to be allied with an almost immediate impact on the Centre's internal structure and organization. As a result, the CNCS carried out identification processes to whom Article 2 refers to, mainly OES and DSP, which are continuously being updated (Portuguese Official Journal, 2018).

Under article 15 of the implementation, public administration and critical infrastructures operators notify the CNCS of incidents with relevant impact on NISs, within a timeframe specified by the applicable legislation (Portuguese Official Journal, 2018). The notification process also includes information that allows the CNSC to determine the cross-border impact of such an incident: whatever are the circumstances, the Centre must provide the notifier with relevant material that may contribute to an efficiently treatment of the incident. According to I1, the Centre was later responsible for the creation of the National Framework of Reference for Cybersecurity (QNRCS), aligned with Directive (EU) 2016/1148, a mechanism that facilitates national organizations to reduce the risk associated with cyberthreats, by stimulating private and public cooperation's awareness on the topic without causing substantial costs or liabilities

to the companies, focusing mainly on risk management techniques and habits (CNCS, 2019). The QNRCS is available on the CNCS official website and presents itself as a complementary product for the Centre to provide references and support tools (ibid.).

3.6- The transposition of the GDPR and additional projects

With the implementation of the GDPR in 2018, great concerns were laid upon the MSs, especially regarding the transposition to national law. Even though the document became applicable all across the Union, it opened at the same time space for the MSs to specify some of their own rules. In other words, it meant that the countries, within certain limits, could maintain or adopt national provisions to specify the application of the GDPR rules itself (Mota & Sampaio, 2019). The GDPR insofar worked as a culmination of a legislative process that showed that the EU wanted a united front for the defence of citizen's personal and digital data: "the regulation is yet another mechanism for European sovereignty, one that works as a whole and not State by State" (I2).

At the time, Portugal fell short as the formulation of a national legislation was still practically nonexciting. According to the Portuguese Association for the Development of Communications (2019), the country, in 2019, alongside Greece and Slovenia, received harsh criticism for being the remaining EU-Member States to not go in accordance with the requirements made by the EU – as it is highlighted on preamble 8 of Regulation (EU) no. 2016/679. The reasons for such delay were justified with incongruences between the political parties with parliamentary seat and the National Commission for Data Protection (CNPD), that accused the Government of not having enough human resources – an issue that has been prevalent throughout the years. A journalistic source (I2) confirms that the CNPD had no sufficient means in order to apply these new rules affectively, showing that Portugal did not have the necessary technical competence to implement and guarantee equal rights to all citizens and companies.

In fact, the same source confirms that it was not the CNPD's fault. "Portugal was delayed, yes" (I2), but it was mainly due to the "lack of initiative and political willingness from the State in guaranteeing that this process would be attended to with time and patience" (ibid.). I2 also highpoints how the Government in office only presented a law-proposal regarding legal matters that the State could legislate in February of 2018. This scarcity of political action also left a mark two years later, where CNPD's resources and structure still have not been properly modernized and solidified: "A restructured CNPD

would allow a much better application of the GDPR, but that is something the CNPD itself may have some reluctance, taking into account that would apply organic changes and internal restructuring" (I2).

However, I2 still considers the country's lateness a transversal opinion, one that tends to oscillate between lawmakers and other political figures. Until the implementation of the GDPR, there were some Government initiatives, at a national and transnational level, that allowed citizens and businesses to know that new standards and set of rules were going to exist. Awareness campaigns and workshops were also held and media coverage, although slightly overshadowed by other topics, remained consistent[31].

Yet, in practical terms, the GDPR continues to show some technical gaps that do not allow its effective implementation. When the Portuguese law gained force, national bodies were still having trouble settling it in. With the applicability within national borders, through Law no. 58/2019, in 2019, the CNPD announced that it would disapply nine articles of the national legislation, namely the ones concerning paying fines during a three-year time spam, renewal of consent practices, administrative offenses, the right to secrecy, and many others. (Machado, 2019). Among them, article 20º was not applied, considering that there was a legal restriction unfounded to the exercise of the data holder's rights (Mota & Sampaio, 2019). Article 28º was disapplied because it harmed excessively workers' consent in a way that could limit their free will in any work-related environment (ibid.). And in this sense, article 37º and article 38º were inapplicable due to their contradicted the infractions' taxing list foreseen in the GDPR and their respective sanctioning framework (ibid.). These are only a few examples that were strictly and quickly circumvented. Through Deliberation no. 2019/495, the CNPD later justified that these norms of the Regulation were "manifestly incompatible with EU law", informing that disapplying them in future cases that would eventually deal with the treatment and processing of personal data, as well as the conduct of the responsible actors involved (CNPD, 2019). The CNPD also considered that some rules could not be saved by "corrective interpretation" in accordance with EU law for its "antinomy with the GDPR rules and the EU's Charter of Fundamental Rights" (CNPD, 2019: 1).

The topics of video surveillance and age consent also created several concerns among MS, including Portugal, and were pinpointed by I2. About the former, it gained relevancy

[31] National newspapers like Observador, SAPO, Público, Expresso and Diário de Notícias maintained the topic of the GDPR implementation relatively active, creating specific tags that were updated frequently, and dedicating more in-depth news on the topic.

at a time when some States were trying to start using large-scale smart cameras that automatically allow data collection[32]. According to the source, the issue has created a problem of collision of rights by wanting, on one hand, the protection of citizens' data, but, on the other, the application of this type of technology in various public places. To this extent, Law no. 58/2019 establishes the prohibition on cameras focusing on public roads, ATM spaces, sanitary facilities or other areas reserved for customers or users' privacy, the interior of areas reserved for workers, etc. (Portuguese Official Journal, 2019). Whereas the later, at a time when young people are increasingly accessing online platforms, the correct application of the GDPR could greatly compromise the fluid use of numerous mechanisms and online tools; so, by activating a *stricto sensu* of what the Regulation demands for companies, it could cause irreversible damage. Because of that, Portugal decided to adopt the digital age of consent at 13, and until then, the treatment of the child's data was only complied if permission were given by the legal guardians, preferably with recourse means of securing authentication (ibid.: 10).

During this period, and facing present constraints, some Portuguese deputies of the EP delivered a written request to the European Commission, asking for a clear understanding of what norms should or should not be applied, giving great matter to a full and effective validity of the GDPR in Portugal. The Commission's answer was ambiguous, stating that an evaluation of national laws was taking place, but postponing at the same time a bilateral dialogue between the two parties in order to measure possible solutions (Mota & Sampaio, 2019). While the Commission speaks overall of a positive result regarding the first year of the Regulation's application, there were still some grey areas to attend to. According to a communication from the Commission to the EP and the Council, the implementation of the legal framework was inconsistent throughout the various MB, and addresses such fact as a "matter of urgency" (EP and the Commission, 2019: 18). The document does not directly mention Portugal as an example *per se* – it explicitly refers to "three Member States which have not yet updated their national data protection law" (ibid.: 18). However, like it was mentioned before, it is easy to understand that the country was overdue when it came to the GDPR's complementation.

As a form of compensation, the Commission laid out indications in order to help these MSs reach their full potential; one of them was directed to the respective data protection

[32] Shao, Z., Cai, J. & Wang, Z. (2017) Smart Monitoring Cameras Driven Intelligent Processing to Big Surveillance Video Data. *IEEE Transactions on Big Data,* 4(1), pp. 105-116.

authorities and to their ability to establish joint investigations and enforcement measures. The main objective is to mitigate resources' constrictions and promote cooperation, like it is stated on article 61 of the GDPR (ibid.; EP and Council of the EU, 2016).

In Portugal, since the passing of the law in 2018, there have been carried out joint investigation projects, happening at both national and international level. According to the CNPD annual report of 2018, one of the goals set was to work close with other WGs for the implementation of the new European legal framework designed for the protection of personal data, notwithstanding an active participation with national institutions, such as the CNSC, the GNS, the Ombudsman, and some Academic Centres (CNPD, 2018). The document was produced and divulged as a way of showcasing Portugal's improvements in the context of designing and developing new mechanisms for information systems, as well as new notification and communication procedures. And while it did not mention any kind of pressure from the EU, it subtly referred to a uniform "application of the new legal regime without endangering the specifics of our constitutional law" (ibid.: 2). Similarly, it raised attention to the creation of specific guidelines by the CNPD to guarantee fundamental rights to citizens, companies and public bodies to create conditions for the application of that regime. These new procedures were also extended oversees, providing assistance to Portuguese-speaking regions, like Macau and Cape Verde, promoting subsequently the creation of a larger and more participative data protection network (ibid.).

But the international cooperative plans of action also extended themselves to other institutions – mainly European ones. The CNPD, in 2018, worked vigorously with tasks provided by EUROPOL, the EDPB, the International Telecommunication Union (ITU), the Customs Information System Supervisions Coordination Group (CIS SCG), and many others to ensure a constant dialogue with EU bodies. On the document, it was not very easy to identify the functions the CNPD had throughout these processes, since the explanations for each group are rather simplistic and brief. In one way or another, most of the descriptions presented end up paraphrasing one another, depending on arguments from the creation of documents that pointed out the latest technological developments, to the repeated importance of personal data protection and the transition to the new Regulation by betting on European cooperation and coherence (ibid.).

The 2019 report did also not show big changes in establishing new goals, nor detailing what was accomplished within the time frame of a year. In fact, most of the bullet points presented in the previous paragraphs were duplicated in last year's report. There were,

evidently, solid changes – namely when approaching new legislative guidelines – that stood out on their own (CNPD, 2019). The first one was about the registration of activities provided for in article 30 of the GDPR (about the records of processing activities), that showed how the Commission helped companies and public bodies during the transition period with essentials practical guidelines in the form of activity registration templates. The second one was about energy consumption and how industries can process personal data and make a smart use of energy distribution networks. The third and final one was about political marketing – in a year marked by the Portuguese legislative elections –, specifically in providing distinctive guidelines to prevent or lessen the impact of misleading information not only on privacy data subjects, but as well as on the functioning of the democratic system (ibid.).

Adjacently, a number of other external laws and conventions stood out at this time, mainly from the EP, and were applied in the context of cybercrime. One of them was the Directive 2016/680/EU on the protection of natural persons' data by competent authorities for "the purposes of the prevention, investigation, detection or prosecution of criminal offences", not forgetting free circulation of such data. This document was incorporated in the so-called Data Protection Package by the EU – that also included the GDPR –, and therefore aimed to protect personal data and the rights of its holders, ensuring compliance with the MSs and their own regulatory treatment of personal data (EP and the Council, 2016). Even though the Commission assisted the MSs, in order to facilitate a correct and timely transposition, through dedicated websites and guidance documents, as well as through the exchange of best practices at WGs' meetings, the MSs failed at transposing these EU rules into national law on time (Enterprise Europe Network, 2019). Portugal was an example of late application due to certain restraints. Analysing a document from the CNPD about Directive 2016/680, under Proposition of Law no. 125/XII/3ª, the Centre once again had issues with the proposal under review. And while it complimented the positive aspects the national legislature had in achieving new improvements that were not essentially provided on the Directive – it still referred to some conclusions that appeared to have harmful interpretative risks for the correct transposition, as well "as for the full respect of rights, freedoms and guarantees of data subjects" (CNPD, 2018: 17).

The document provided an outlook that reflected the lack of resources (previously mentioned) and interpretations the CNPD had with the Directive. But most importantly, it confronted the legislator with how it would affect the compositional body of the Centre

and the functions of some of its members: "[…] to replicate the implicit suggestion that only magistrates will be able to perform some of the competences attributed to CNPD" (ibid: 18). In the same statement, the term "disrespect" was used to showcase the main position of the Centre, concerning the status of equality shared among them.

In midst of implementing the GDPR, the Portuguese population reacted with animosity, which ended up complicating the integrational process and building restraints in awareness campaigns. According to a paper from the Portuguese Ministry of Economy on Cybersecurity, Portugal ranked among the EU as one of the countries that feel less secure in sharing personal data and contact information on the internet (48,6% and 15,2% respectively, when compared with 71,4% and 61,1% of the UE) (Ministry of Economy, 2018). At this rate, it occupied the 21th position, of a list of 24 countries whose population feel indeed secure in providing private details about home address, phone number, full name, date of birth, and etc (ibid.).

Chapter 4 – Discussion: Portugal's position regarding cybersecurity on the EU map and onwards

In comparison with other European countries, Portugal occupied the second place, only behind Sweden, in registered cases of privacy violation, between 2010 and 2015, that resulted in malicious activities and loss of vital information (ibid.). During the same period, 24,6% of Portuguese citizens confirmed being victims of cybersecurity incidents, as it is showed in Annex II of this Dissertation. The same report showed that these types of occurrences mostly happen to people with higher educational degrees or when the usage of ICTs is more frequent.

We can analyse that the position Portugal faced at the time was worrisome, as the population still was not fully aware of how to identify and prevent a cyberattack, as well as protect themselves from it (CNCS, 2019). I1 looks at cybersecurity as a whole and associates the growing number of incidents to "human and/or technological causes". However, according to the same source, the simplification of such statements is itself a risk: in his words, there is a substantial difference between people that were consciously victims of a cyberattack and those, that during the process, were unaware of it. This means that the perception of a population may actually mean less detection capacity and not necessarily fewer security incidents affecting individuals in this context: "if so, we are still talking in the field of hypotheses" (I1).

While confronting this reality, national authorities were eager to change the direction and take a sturdier step in combating cyberthreats. Like so, Decree-Law noº 81/2016 saw the creation of a special unit, the National Unit to Combat Cybercrime and Technological Crime (UNC3T)[33], dedicated to cybercrime and cyber prevention, that enjoys technical and scientific autonomy (Portuguese Official Journal, 2016). Its main responsibilities were based on the prevention, detention, criminal investigation and assistance of the judicial authorities in relation to online crimes, not excluding any form or means of crimes committed using computer technology (Antunes & Rodrigues, 2018). This unit was also accountable for testing and developing specific procedures and methodologies for the investigation of technological crime: from establishing cooperation ties with international police forces, to ensuring regular functioning of an informal and national advisory group

[33] In Portuguese, referred to as the Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica.

for strategic, legal and scientific debate on issues related to cybersecurity – that can also provide assistance to companies or personal entities (ibid.).

Beforehand, there already was a unit specialized in fighting terrorism, the National Unit Against Terrorism (UNCT)[34], embedded in the Judiciary Police (PJ) formation. However, the two combined forces because of Decree-Law nº 81/2016, and further gained new tasks and goals – such as updating the National Plan of the PJ for the Prevention and the Fight against cybercrime, in articulation with CNCS, too. This Decree-Law also saw the reinforcement of previous legislative documents, more specifically Decree-Law no. 109/2009, that was defined as the "Cybercrime Law" (Portuguese Official Journal, 2016), whose emergence came as a way of accommodating a reality in which the scope of crimes and scams involving computer equipment and electronic devices gained prominence (Antunes & Rodrigues, 2018).

On article 33 of Decree-Law no. 137/2019, regarding a new organizational structure of the PJ, the UNC3T gained regulations that were extended from the original document. Besides the working under the directions that were previously mentioned, the Unit started to centralize the treatment of criminal information related to espionage, sexual freedom, self-determination, computer fraud and interference, as well as illegitimate manipulation of electronic and virtual means of payment (Portuguese Official Journal, 2019). It also became responsible for handling and collecting statistical data and creating protocols of technical and scientific nature with public and private entities, regardless of being national or foreign, but with prior approval from the National Board of Management (ibid.).

Since the first years of its creation, the UNC3T participated in WGs supported by EUROPOL in matters of cybersecurity resilience, creating, alongside other members of the EU, the European Cybercrime Task Force (EUCTF), that received constant support from the European Commission. This platform managed cybercrime investigations and prosecutions, while assisting problems caused by the use of cyber technology for unlawful purposes. The Portuguese participation was a bit one-sided and resourceless at first, but throughout the years, the scenario changed (Sistema de Segurança Interna, 2016). By 2019, according to a document published in the same year by the Office of the Secretary-General of Homeland Security System, the national Unit enlarged its field of action and started providing support to non-European countries, mostly Portuguese-speaking ones: among several other examples, it developed workshops and seminars in

[34] In Portuguese, referred to as the Unidade Nacional Contra o Terrorismo.

Angola, created and supervised academic courses in Brazil, and opened dialogues with the Mozambican National Criminal Investigation Services. All of them related to cybersecurity. (Sistema de Segurança Interna, 2019).

Looking back at the progress made throughout the years, in Portugal, the influence of the EU can be felt in the field of cybersecurity at numerous levels, from legal, administrative and to even technical ones. Although I1 talks about this correlation as sometimes difficult to be distinguished, essentially because of the legislative process, namely the adoption of legislative acts, that is under the responsibility of the Council of the EU and the EP – normally under a proposal from the European Commission. These institutions develop actions with a more operational focus when discussing the implementation of EU policies. The goal is to create better conditions in order to establish cooperation between the stakeholders and between some agencies – with ENISA being a clear example –, in the field of cybersecurity.

In this sense, even if Portugal took some significant steps in the late 1990s with the recognition of privacy and information security as one the essential pillars to accompany the development of national technologies, the same source points out that the main legislative advances in this matter emerged alongside European initiatives, as the EU always presented itself to be a strong figure in providing resources and support to the MB – highlighting such action plans like the creation national alert platforms; the development of large-scale cyberattacks simulation operations; the formation of CERTs and the establishment of national networks of CERTs; the construction, alongside ENISA, of national and European contingency and cooperation plans, in areas of response and disaster recovery; and the organization of outreach seminars, awareness campaigns and technical training directed at the industry and academic sectors; among many others (Santos, 2014).

In Portugal, like it was mentioned throughout this dissertation, the transitional period for European legislation is usually done with delay, in comparison with other MB, and causing some level of constraints among national bodies. On the global strategic plan for rationalization and cost reduction in ICT, from 2012 to 2016, made by the Portuguese Government, the national legal framework for the development of private and industrial communication and information systems was considered “out of date”, and in needing of “a new approach and statue that equates the legal framework” (Portuguese Government, 2011: 42) of other existing nations – namely from the European Union. A possible solution presented in the same document pointed out a coordinated measure

supervisioned by the GNS with the collaboration of all relevant entity for this subject, with every development reported to the ICT Network, within the scope of the existing WGs. (ibid.).

When asked about if there is still an omnipresent sense of pressure made by the EU, I2 swiftly responded: "yes, undeniably". Even though the interviewee was directly talking about the GDPR, he also stated that it can be practically implemented on almost every aspect of the cyber landscape. "The EU is tough negotiator, and a pragmatical case is the tug-of-war that the European Court of Justice was on regarding sanctions", concluded. An important case to observer is how the EU imposed their new regulations in non-European markets. Oversees, the EU Court of Justice made adamant comments on how European data was being handled by the United States, for example, that subsequently made many companies reconsider the way stored and collected the data of European customers, as they were not being restricted in a way that was equivalent to E.U. rules (The Washington Post, 2020). The final say was either by setting up an expensive "Europe-based data hubs or curtailing business in Europe altogether" (ibid.). A final outcome is still to be designed by the end of this academic paper.

Within national borders, by 2019, there were already registered four occasions the CNPD had to impose fines. Three of them were to private companies, whose identify was never fully revealed, because of specific information a citizen wanted to consult but permission was never given or the access was eliminated (ECO, 2019). The remaining one happened, in 2018, in a public Hospital, in Barreiro, that was fined 400 000 euros by the CNPD, for allowing irregular access to a patients' data. One of the violations found was the "indiscriminate access" to data by professionals that should only be able to access it in specific cases. The second violation committed by the Hospital was in showing inability to "ensure the confidentiality, integrity, availability and permanent resilience of working systems and services" (Lusa, 2018).

According to both sources and to the research made throughout this dissertation, we can conclude that, besides the setbacks and certain limitations, Portugal is concentrating on a technological development[35] that reaches the most diverse areas of business and entrepreneurship. And despite cybersecurity is far from being at the top of the agenda for the Lusophone world (Ministry of Economy, 2018), the country still plays a key-figure

[35] eco.pt, *Portugal no 'Top20' europeu de talento e investimento tecnológico*, [online]. Available at: https://eco.sapo.pt/2020/02/04/portugal-no-top20-europeu-de-talento-e-investimento-tecnologico/ (Accessed: 9th November, 2020).

for the EU's Digital Economy and has been showing improvements regarding cyber matters. For once, it is worth mentioning the creation of a cyber-resilience laboratory by COTEC Portugal in 2018, with the objective of bettering the identification of main weaknesses in terms of governance, defence and reaction procedures and technologies. I2 visions a confident vision of the future principally thanks to a new adopted National Cyberspace Security Strategy 2019-2023 (ENSC 2019-2023), formulated by a Government-appointed group in 2017, and approved through Resolution no. 92/2019. The elaboration of this Action Plan resulted in the purpose of making "Portugal a safe and prosperous country through and innovative, inclusive and resilient action that […] guarantees the regular functioning of the institutions in the face of the digital evolution of society". (Portuguese Official Journal, 2019: 2). In other words, it aimed to deepen the security of networks and information systems and to ensure a free and efficient use of the cyberspace by all citizens. The CNCS were attributed the responsibility of coordinating and monitoring the ENSC implementation and review in articulation with all institutional bodies that operate within the domain of cybersecurity.

I1 also notes that one of the CNCS's concerns is, while being a body of advisory nature to the Prime Minister, the proper verification of the ENSC's implementation, not forgetting the elaboration of an annual report in order to evaluate the success of such execution – much like it is proposed on Law no. 46/2018. For its completion, the Strategy worked mainly on three strategic objectives: the maximization of resilience, by enhancing inclusion and network collaboration in the presence of threats that could compromise or cause the disruption of network and information systems; promoting innovation by potentializing national cyber capacity in cultural, social, technological and economic domains; and, finally, to manage and secure resources, by contributing to assurance the allocation of resources suitable for constructing and supporting the national capacity for cybersecurity that may go in accordance with European standards (ibid.). The document provided as well new reinforcements for CERT.pt, the national Security Information Service, the PJ's capacities and an upgrade of the organizational structures of the Public Prosecutor Office (ibid.). As a result, the CNCS counts on already recording new changes and impacts on the Portuguese society during the elaboration of their next annual report for Cybersecurity in Portugal.

Conclusions

In this work, we proposed to study how the EU has impacted Portugal's internal organization regarding cybersecurity procedures, documenting the major steps taken by the Union, and how the country responded to them respectively.

The creation of ENISA in 2004 served as a catalyst process for the uniformization of the EU's position regarding cybersecurity in order to achieve the idealization of a "pan-European cyber" community (Markopoulou et al., 2019). Quickly after, various EU Members started developing their own cyber strategies – and even though this procedure took irregular turns, ENISA eventually became the ultimate body of cooperation, spreading institution-building among the MSs. One of the most critical measurements proposed by the Agency was indisputably the establishment of CERTs as a way of preparing the countries for the increasement of cyberthreats, as well as ensuring a stronger and more active level of communication among European teams. Afterwards, cornerstones moments like the implementation of the NIS Directive, the GDPR, more recently the Cybersecurity Act, among others, served to prove the EU's position shaping the domestic organization of its Members, while maintaining a multi-level governance model. Cavelty (2018) abords the EU's plan of action as a superlative way of safeguarding protection, but also stresses the difficulty some member had in securing their respective networks with their own knowledge and available tools.

That is when the concept of Europeanization pierces the analysis of this dissertation: an "incremental, irregular and uneven" (Featherstone, 2003: 4) process that bends time and locations, and represents "how public administrative institutions […] have adapted to the obligations of EU membership" (ibid.: 7). For a better understanding of this concept, it is pivotal to highlight the historically-driven debate between neofunctionalism and intergovernmentalism. When approaching cybersecurity policies, the predictions of the first one hasn't been totally outdated: there is still no doubt that integration in a specific policy area will lead to spill-over into another (Dunn, 2012), as European processes may trigger others and bigger integrational ones. On the other hand, intergovernmentalism argue that the state plays a more central role in foreign policies, rejecting the spill-over effect. Dunn (ibid.) concludes by saying that before an increase in power for supranational institutions, there are decisions made from the governments. Regarding cybersecurity, it's more difficult to avoid policy spill-overs and integration over the years will be proven as a current method for the EU.

While approaching Portugal, the climbing of EU's steps was made at a not equal manner when compared to other MSs. By the early 2000's, the country still did not have a functioning computer response team. In addition, it applied the diligences of the Budapest Convention eight years later. It was one of the last countries to establish a physical a national cybersecurity centre. And it transposed the GDPR regulation with delay while suffering limitations from its national body.

However, it is positive to affirm that the country has two Europeanization processes on its structural DNA. The first one is the participation of Portugal in EU WGs, conventions and committees, as well as establishing frequent contact points with ENISA and other MSs. Our study observes how these interactions shaped, more or less, the domestic structure of the country; yet, the language it presents, especially after conducting an interview with a Government official, is rather dubious and still based on diplomatic platitudes. According to the scale made by Börzel and Risse (2009), the degree of domestic change is "absorption". The second example is more practical and details the EU's influential decisions in the political foreground of the country, as it adopted, at its own time, new regulations that affected the internal organization. We can classify the latter as an example of "accommodation", but with a small touch of "transformation", because of how incommensurable the GDPR was on national policy and how it changed the way (not only) Portuguese citizens and entities viewed data.

It is also important to address that, throughout the making of this dissertation, there were some complications that limited the work itself. The first one was the congregation of information, specially about Europeanization: not only did the finding that we gathered were not from one or two years ago – despite some exceptions –, but my efforts to find literature that linked the topic of Europeanization to cybersecurity was difficult and almost resulted in nonexciting outcomes. Another struggle was the time in which this dissertation was made: taking in consideration that the COVID-19 pandemic caused awful and crucial problems worldwide, it difficulted the way the interviews were conducted. Last but not least, the topic of cybersecurity itself was difficult to work on, since it is constantly getting upgraded and being revisited, particularly in a small country like Portugal. However, that is also the most interesting part: the handling of current data that could propel the study of numerous research projects, from the final results of ENSC 2019-2023 to the analysis of future legislations in Portugal.

Sources

ANACOM, (1998). Resolução do Conselho de Ministros no. 115/98. September, 1st, Lisbon

APDC, (2019). *UE adverte Portugal por não legislar sobre proteção de dados* [online]. Available: http://apdc.pt/noticias/atualidade-nacional/ue-adverte-portugal-por-nao-legislar-sobre-protecao-de-dados (Accessed: November 11th. 2020)

Barros, G. (2018). *A Cibersegurança em Portugal.* Ministério da Economia, August, Lisbon

Birnbaum, M. (2020) "Top E.U. court ruling throws transatlantic digital commerce into disarray over privacy concerns", *The Washington Post* [online]. Available: https://www.washingtonpost.com/world/europe/top-eu-court-ruling-throws-transatlantic-digital-commerce-into-disarray-over-privacy-concerns/2020/07/16/d2c0fe06-c736-11ea-a825-8722004e4150_story.html (Accessed: November 12th. 2020)

CNCS, (2019). *Governo aprova nova Estratégia Nacional de Segurança do Ciberespaço* [online]. Available: https://www.cncs.gov.pt/recursos/noticias/governo-aprova-nova-estrategia-nacional-de-seguranca-do-ciberespaco/ (Accessed: November 3rd. 2020)

CNCS, (2019). *Quadro Nacional de Referência para a Cibersegurança* [online]. Available: https://www.cncs.gov.pt/content/files/cncs_qnrcs_2019.pdf (Accessed: November 10th. 2020)

CNCS, (2019). *Relatório: Cibersegurança em Portugal.* Observatório de Cibersegurança

CNCS, (not identified). *Coordenação da Resposta a Incidentes* [online]. Available: https://www.cncs.gov.pt/certpt/coordenacao-da-resposta-a-incidentes/ (Accessed: November 3rd. 2020)

CNCS, (not identified). *Rede Nacional de CSIRT* [online]. Available: https://www.cncs.gov.pt/cooperacao/rede-nacional-de-csirt/ (Accessed: November 3rd. 2020)

CNPD, (2018). *Parecer no. 24/2018*. Lisboa. Comissão Nacional de Proteção de Dados

CNPD, (2018). *Plano de Atividades CNPD 2018.* Lisboa. Comissão Nacional de Proteção de Dados

CNPD, (2019). Deliberação 2019/495 [online]. Available: https://www.cnpd.pt/home/decisoes/Delib/DEL_2019_495.pdf (Accessed: November 14th. 2020)

CNPD, (2019). *Plano de Atividades CNPD 2019.* Lisboa. Comissão Nacional de Proteção de Dados

Comissão Europeia, (2010). *Comunicação da Comissão ao Parlamento Europeu e ao Conselho. Estratégia de Segurança Interna da UE em ação: cinco etapas para uma Europa mais segura.* Bruxelas: COM(2010) 673 final

Council of Europe, (1989). *Recommendation no. 89/9 of the Council of Europe and the Committee of Ministers on Computer-Related Crime*. Brussels.

Council of the EU, (2001). *European Treaty Series – no. 185. Convention on Cybercrime.* Budapest

Council of the EU, (2008). Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, *Official Journal*, L345, pp. 1-8

Diário da República, (1996). Resolução do Conselho de Ministros no. 16/96. February 26th, Lisbon

Diário da República, (2012). Resolução do Conselho de Ministros no. 12/2012. February 7th, Lisbon

Diário da República, (2012). Resolução do Conselho de Ministros no. 42/2012. April, 13th, Lisbon

Diário da República, (2013). Despacho no. 13692/2013. October 28th, Lisbon

Diário da República, (2013). Resolução do Conselho de Ministros no. 19/2013. April 5th, Lisbon

Diário da República, (2014). Decreto-Lei no. 69/2014. May 9th, Lisbon

Diário da República, (2015). Resolução do Conselho de Ministros no. 36/2015. June 12th, Lisbon

Diário da República, (2016). Decreto-Lei no. 81/2016. November 28th, Lisbon

Diário da República, (2018). Lei no. 46/2018. August 13th, Lisbon

Diário da República, (2019). Decreto-Lei no. 137/2019. September 13th, Lisbon

Diário da República, (2019). Lei no. 58/2019. August 8th, Lisbon

Diário da República, (2019). Resolução do Conselho de Ministros no. 92/2019. June 5th, Llisbon

Direção-Geral de Estatísticas da Educação e Ciência, (2011). *Plano global estratégico de racionalização e redução de custos nas TIC, na Administração Pública.* Governo de Portugal, Lisboa

ENISA, (2005). *ENISA General Report 2005.* Greece, European Union Agency for Cybersecurity

ENISA, (2006). *WG 2006-2007* [online]. Available at: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/working-group/wg-2006-2007 (Accessed: September 3rd. 2020)

ENISA, (2007). *ENISA General Report 2007.* Greece, European Union Agency for Cybersecurity

ENISA, (2012). *ENISA Annual Incident Report 2012.* Greece, European Union Agency for Cybersecurity

ENISA, (2019). *Cybersecurity Skills Development in the EU.* Greece, European Agency for Cybersecurity

ENISA, (2019). *ENISA Annual Activity Report 2019.* Greece, European Union Agency for Cybersecurity

ENISA, (2019). *NIS Cooperation group and knowledge building meetings concluded in Athens* [online]. Available: https://www.enisa.europa.eu/news/enisa-news/nis-cooperation-group-and-knowledge-building-meetings-concluded-in-athens (Accessed: September 17th. 2020)

ENISA, CERT-EU, EUROPOL & European Defense Agency, (2018). *Memorandum of Understanding between The European Agency for Network and Information Security (ENISA) of the first part, The European Defence Agency (EDA) of the second part, EUROPOL's European Cybercrime Centre (EC3) of the third part and the Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (CERT-EU) of the fourth part.* May 23rd. 2018

Enterprise Europe Network, (2019). *Cumprimento do direito da UE pelos Estados-Membros em 2018* [online]. Available: https://www.een-portugal.pt/news/Paginas/Cumprimento-do-direito-da-UE-pelos-Estados-Membros-em-2018.aspx (Accessed: November 17th. 2020)

European Commission, (2006). *European Court of Justice confirms legality of the establishment of the European Network and Information Security Agency* [online]. Available at: https://ec.europa.eu/digital-single-market/en/news/european-court-justice-confirms-legality-establishment-european-network-and-information-0 (Accessed: September 5th. 2020)

European Commission, (2013). *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Brussels: JOIN(2013) 1 final

European Commission, (2017). *Commission Staff Working Document Assessment of the EU 2013 Cybersecurity Strategy.* Brussels: SWD(2017) 295 final

European Commission, (2017). *Commission Staff Working Document Impact Assessment Accompanying the document: Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) no. 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act").* Brussels: SWD (2017) 500 final

European Commission, (2018). *Cybersecurity Act* [online]. Available at: https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en (Accessed: September 11th. 2020)

European Commission, (2018). *NIS Cooperation Group's Guidelines for implementing the NIS Directive and addressing wider cybersecurity policy issues* [online]. Available: https://ec.europa.eu/digital-single-market/en/news/latest-nis-cooperation-group-guidelines-for-implementing-nis-directive (Accessed: September 17th. 2020)

European Commission, (2018). *Questions and Answers: Directive on Security of Network and Information systems, the first EU-wide legislation on cybersecurity [Updated on 28/10/2019]* [online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3651 (Accessed: September 8th. 2020)

European Commission, (2019). *Communication from the Commission to the European Parliament and the Council.* Brussels: COM(2019) 374 final ~

European Commission, (2019). *Report from the Commission to the European Parliament and the Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems.* Brussels: COM(2019) 546final

European Commission, (2020). *Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation.* Brussels: COM(2020) 264 final

European Commission, (2020). *NIS Cooperation Group* [online]. Available: https://ec.europa.eu/digital-single-market/en/nis-cooperation-group (Accessed: September 17th. 2020)

European Commission, (2020). *The Directive on security of network and information systems (NIS Directive).* [online]. Available at: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive (Accessed: September 7th. 2020)

European Court of Auditors, (2019). *Challenges to effective EU Cybersecurity Policy Briefing Paper.* European Union

European Parliament and Council of the EU, (2004), Regulation no. 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (1999) *Official Journal,* L77, pp. 1-11

European Parliament and Council of the EU, (2016). Directive 2016/1148 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, *Official Journal,* L194, pp. 1-30

European Parliament and the Council of the EU, (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of

individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal of the European Communities*, L281, pp. 31.50

European Parliament and the Council of the EU, (2012). Consolidated version of the Treaty on the Functioning of the European Union. *Official Journal*, C326, pp. 47-390

European Parliament and the Council of the EU, (2016). Directive 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 by competent authorities for the purposes of the prevention, investigation, detection or persecution of criminal offences or the execution of criminal penalties, and on the free movement of such data and repealing Council Framework Decision 2008/977/JHA. *Official Journal*, L119, pp. 89-131

European Parliament and the Council of the EU, (2016). Regulation no. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *Official Journal*, L119, pp. 1-88

European Parliament and the Council of the EU, (2017). *Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.* Brussels: JOIN(2017) 450 final

European Parliament and the Council of the European Union, (2019). Regulation no. 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) no. 526/2013 (Cybersecurity Act), *Official Journal*, L151, pp. 15-69

European Parliament, (2019). *ENISA and a new Cybersecurity Act.* [online]. Available at:https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf (Accessed: September 14th. 2020)

European Parliament, European Commission, European Council, European Economic and Social Committee & European Committee of the Regions, (2001). *Network and Information Security: Proposal for a European Policy Approach*. Brussels: COM(2001) 298 final

European Union Global Strategy, (2016). *Shared Vision Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy* [online]. Available: https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf (Accessed: September 8th. 2020)

General Secretariat of the Council, (2016). *European Council Meeting (15 December 2016) – Conclusions*. European Council

General Secretariat of the Council, (2017). *Final report of the seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating cybercrime"*. Brussels: REV2 (2017)

General Secretariat of the Council, (2019). *Preparation of the Council position on the evaluation and review of the General Data Protection Regulation (GDPR) – Comments from Member States.* Brussels: REV1 (2019)

Lusa, (2018) "Hospital do Barreiro contesta judicialmente coima de 400 mil euros de Comissão de Dados", *Público* [online]. Available: https://www.publico.pt/2018/10/22/sociedade/noticia/hospital-barreiro-contesta-judicialmente-coima-400-mil-euros-comissao-dados-1848479 (Accessed: November 12th. 2020)

Machado, M. (2019) "Portugal aprova lei de proteção de dados um ano depois do RGPD", *Observador* [online]. Available: https://observador.pt/2019/06/14/portugal-aprova-lei-de-protecao-de-dados-um-ano-depois-do-rgpd/ (Accessed: November 12th. 2020)

Nunes, F. (2019) "Já houve quatro multas em Portugal por causa do RGPD. Uma foi ao Hospital do Barreiro e três a empresas privadas", *Eco* [online]. Available: https://eco.sapo.pt/2019/05/17/ja-houve-quatro-multas-em-portugal-por-causa-do-rgpd-uma-foi-ao-hospital-do-barreiro-e-tres-a-empresas-privadas/ (Accessed: November 12th. 2020)

Procuradoria-Geral Destrital de Lisboa, (2009). Lei no. 109/2009. September 15th, Lisbon

Santos, D. (2014). *A Cibersegurança em Portugal: A Ação Política Nacional em Matéria de Cibersegurança*, Master Thesis in Public Policies, Lisbon, ISCTE-IUL

Sistema de Segurança Interna, (2016). *Relatório Anual de Segurança Interna 2016.* Gabinete do Secretário-Geral, Lisboa

Sistema de Segurança Interna, (2019). *Relatório Anual de Segurança Interna 2019.* Gabinete do Secretário-Geral, Lisboa

Tribunal da Relação de Lisboa, (2013). *Processo 581/12.6PLSNT-A.L1-5. Lei do Cibercrime* [online]. Available: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/7bd2dd8af10b34c380257b27003a5697?OpenDocument (Accessed: September 14th. 2020)

Bibliography

Aleksandrowicz, T. (2020). The Act on the National Cybersecurity System as an Implementation of the NIS Directive. *Internal Security,* 12(1), pp. 179-193.

Antunes, M. & Rodrigues, B. (2018). *Introdução à Cibersegurança.* 1st edn. Lisbon: FCA – Editora de Informática.

Borneman, J. & Fowler, N. (1997). Europeanization. *Annual Review of Anthropology,* 26(1), pp. 487-514.

Börzel, T. & Risse, T. (2009). Conceptualizing the Domestic Impact of Europe. *Oxford University Press,* 1(1), pp. 20.

Börzel, T. (2002). Member States Responses to Europeanization. *Journal of Common Market Studies,* 40(2), pp. 193-214.

Bowen, G. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal,* 9(2), pp. 27-40.

Bulmer, S. (2008). Theorizing Europeanization. In: M. Vink, & P. Graziano, ed., *Europeanization,* 1st ed. London: Palgrave Macmillan, pp. 46-58.

Carrapico, H. & Barrinha, A. (2018). European Union Cyber Security as an Emerging Research and Policy Field. *European Politics and Society,* 19(3), pp. 299-303.

Carvalho, J., Carvalho, S. & Rocha, A. (2020). European Strategy and Legislation for Cybersecurity: Implications for Portugal. *Cluster Computing*, 23(1), pp. 1845-1854.

Cavelty, M. (2018). Europe's Cyber-power. *European Politics and Society,* 19(3), pp. 304-320.

Christou, G. (2018). The Challenges of Cybercrime Governance in the European Union. *European Politics and Society,* 19(3), pp. 355-375.

Dunn, T. (2012). Neo-Functionalism and the European Union. *E-International Relationsm* 1, pp. 1-3.

Featherstone, K. (2003). Introduction: In the Name of 'Europe'. In: K. Featherstone, & C. Radaelli, ed., *The Politics of Europeanization*, 2003 ed. New York: New York University Press, pp. 3-26.

Goetz, K. (2000). European Integration and National Executives: A Cause in Search of an Effect? *West European Politics,* 23(4), pp. 211-231.

Graziano, P. & Vink, M. (2013). Europeanization: Concept, Theory, and Methods. In: S. Bulmer, & Lesquene, C, ed., *The Member States of the European Union,* 2nd ed. Oxford: Oxford University Press, pp. 31-54.

Gruber, H. (2019). Proposals for a Digital Industrial Policy for Europe. *The International Journal of Digital Economy, Data Sciences and New Media,* 43(2), pp. 116-127).

Hoofnagle, C., Sloot, B. & Borgesius, F. (2019). The European Union General Data Protection Regulation: What It Is and What It Means. *Information & Communications Technology Law,* 28(1), pp. 65-98.

Ladrech, R. (2002). Europeanization and Political Parties: Towards a Framework for Analysis. *Party Politics,* 8(4), pp. 389-403.

Markopoulou, D., Papakonstantinou, V. & de Hert, P. (2019). The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation. *Computer Law & Security Review,* 35(1), pp. 1-11.

Mota, J. & Sampaio, A. (2019). Regulamento Geral de Proteção de Dados em Portugal – Alguns Apontamentos à Sua Lei de Execução. *Actualidad Jurídica Uría Menéndez,* 53(1), pp. 142-148.

Olsen, J. (2002). The Many Faces of Europeanization. *Journal of Common Market Studies,* 40(5), pp. 921-944).

Radaelli, C. (2000). Whither Europeanization? Concept Stretching and Substantive Change. *European Integration online Papers (EIoP),* 4(8), pp. 1-25.

Radaelli, C. (2004). Europeanisation: Solution or Problem? *European Integration online Papers,* 8(16), pp. 1-23.

Rid, T. (2011). Cyber War Will Not Take Place. *Journal of Strategic Studies,* 35(1), pp. 5-32.

Ruohonen, J., Hyrynsalmi, S. & Leppänen, V. (2016). An Outlook on the institutional Evolution of the European Union Cyber Security Apparatus. *Government Information Quarterly,* 33(2016), pp. 746-756.

Schimmelfenning, F. (2015). Europeanization Beyond Europe. *Living Reviews in European Governance,* 10(1), pp. 5-26.

Silva, J. (2019). Cybersecurity and Cybercrimes in Portugal. *Proceedings of the Digital Privacy and Security Conference,* 1(1), pp. 39-47.

Sliwinski, K. (2014). Moving Beyond the European Union's Weakness as a Cyber-Security Agent. *Contemporary Security Policy,* 35(3), pp. 468-486.

Stone, J. (2012). Cyber War Will Take Place. *Journal of Strategic Studies,* 36(1), pp. 101-108.

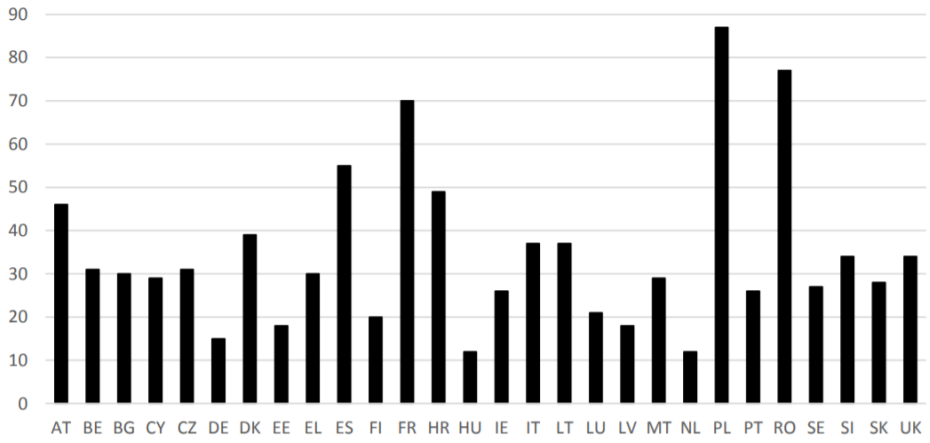
Tömmel, I. (2014). Theorizing European Integration and the Union as a Political System. In: I. Tömmel, ed., *The European Union: What It Is and How It Works (The European Union Series),* 2014 ed. London: Red Globe Press, pp. 10-33.

Vink, M. (2005). What Is Europeanisation? And Other Questions on a New Research Agenda. *European Political Science,* 3(1), pp. 63-73).

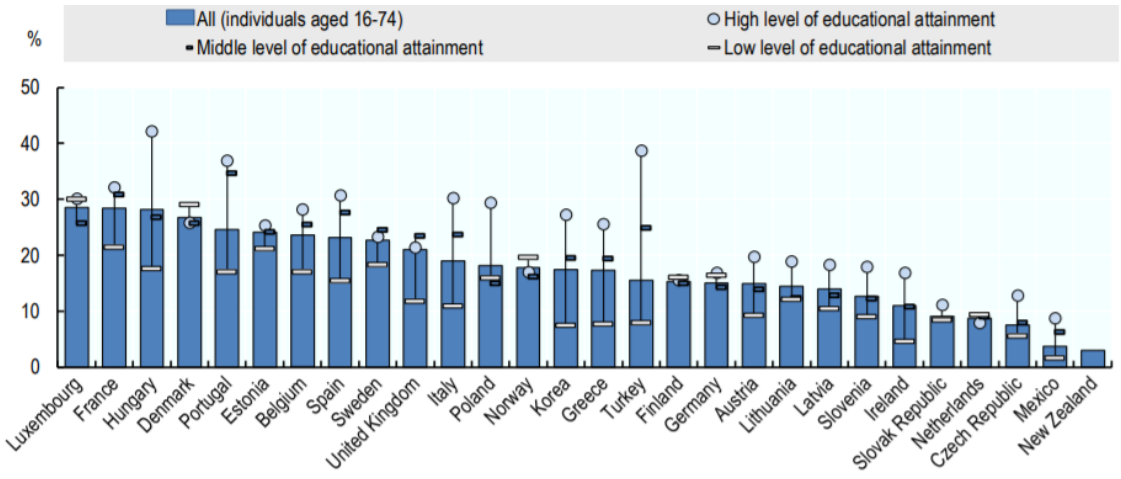
Wallis, T. & Johnson, C. (2020). Implementing the NIS Directive, Driving Cybersecurity Improvements for Essential Services. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment,* 1(1), pp. 1-11.

Wessel, R. (2019). Cybersecurity in the European Union: Resilience Through Regulation? In: Conde. E, Yaneva. Z, Scopelliti. M, ed., *Routledge Handbook of EU Security Law and Policy,* Routledge, pp. 283-300.

Annexes



Annex 1: Overall number of essential services identified by Member States.
Source: Report from the Commission to the European Parliament and the Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems, 2019.



Annex 2: Digital security incidents suffered by individuals in 2015, taking in consideration of all individuals and by the respective level of education.
Source: Ministry of Economy, 2018.

Identification	Respondent	Type of Interview Conducted	Recorded	Additional Information
Interviewee 1 (I1)	Centro Nacional de Cibersegurança	Structured Interview + Questionnaire (via e-mail)	No	The questions were answered by a specific department of the CNCS
Interviewee 2 (I2)	Manuel Pestana Machado at Observador	Semi-structured + Questionnaire (via e-mail)	No	Journalist specialized in technology, whom covered throughout the years the implementation of the GDPR in Portugal

Annex 2: List of interviews conducted.