MYKOLAS ROMERIS UNIVERSITY
SCHOOL OF LAW
INTERNATIONAL AND EUROPEAN LAW INSTITUTE

FAILLIERES DELHALLE LOUIS-PIERRE
EUROPEAN UNION LAW AND GOVERNANCE PROGRAMME

PERSONAL DATA PROTECTION AND NATIONAL SECURITY: EUROPEAN APPROACH

Master thesis

Supervisor –
Prof. Dr. Valutytė Regina

Châtelaillon-Plage, 2023

TABLE OF CONTENT

ABBREVIATION

CFREU: Charter of the Fundamental Rights of the European Union
DMA: Digital Market Act
DSA: Digital Service Act
EC: European Commission
ECHR: Convention for the Protection of Human Rights and Fundamental Freedoms
ECtHR: European Court of Human Rights
CJEU: Court of Justice of the European Union
ENISA: European Union Agency for Cybersecurity
EDPB: European Data Protection Board
EP: European Parliament
EU: European Union
FIMI: Foreign Information Manipulation and Interference
GAFAM: Google-Amazon-Facebook-Apple-Microsoft
GDPR: General Data Protection Regulation
HR: Human Right
MS: Member states
NGO: Non-Governmental Organisation
TEU: Treaty on the European Union
TFEU: Treaty on the Functioning of the European Union
UK: United Kingdom
USA: United State of America
VLOP: Very Large Online Platform
VLOSE: Very Large Online Search Engine

INTRODUCTION

In a very traditional presentation, public order requires limitations to individuals' rights, it is the dialectic: liberty v. security. If, as it will be demonstrated further, national security does limit personal data protection, the exchanges between those two notions are not always conflictual. Sometimes, data protection can be consubstantial to national security, and, today, States have to protect the data of their citizens, not only to ensure this human right, but also for the common good. History has shown that, the enormous quantity of data that people are willing to spread online can be used in various ways, legal or not, to ultimately influence States' politics or even security. To that point, the *Cambridge Analytica* case has shown that competent companies can process data from social media to target persons, qualified as influenceable, for the interests of the highest bidder[1]. This latter, if it can be a candidate for the election — and even though it is already a matter of concern for democratic societies — can also be a much more problematical actor: suspicions of foreign influence have been raised in the Brexit referendum, or US presidential election in 2016[2]. These cases can be attached to what the European Union (hereinafter: "EU") Agency for Cybersecurity (hereinafter: "ENISA") defined in its 2023 *Threat Landscape Report*: "*Foreign Information Manipulation and Interference*" (hereinafter: "FIMI"). It is defined as "*mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Those who undertake such activity may be state or non-state actors, including their proxies inside and outside their own territory*"[3]. The coordinated processing of personal data and advertising targeting, in order to affect the outcomes of national elections, is a clearly identified as a threat by EU institutions[4], a threat the addressing of which is, unarguably, very important for the future of democracy. Indeed, this case shows how important it

[1] Kaisert, Brittany. 2019. "Targeted My inside Story of Cambridge Analytica and How Trump, Brexit and Facebook Broke Democracy". London (Royaume-Uni De Grande-Bretagne Et D'Irlande Du Nord): HarperCollins Publishers, 2019. Eventually, Facebook signed an agreement to settle the proceedings against it before the tribunal of San Francisco, California, USA, on 22 December 2022. (https://fingfx.thomsonreuters.com/gfx/legaldocs/gkplwwkebvb/12232022facebook_settle.pdf, consulted on 23 December 2023).

[2] Kaisert, Brittany. Targeted My inside Story of Cambridge Analytica and How Trump, Brexit and Facebook Broke Democracy. London (Royaume-Uni De Grande-Bretagne Et D'Irlande Du Nord): HarperCollins Publishers, 2019.

[3] ENISA, 2023, "*Threat Landscape Report*", Report. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023, p110.

[4] European Parliament resolution of 1 June 2023 on foreign interference in all democratic processes in the European Union, including disinformation (2022/2075(INI)) (2023). Par.11. http://data.europa.eu/eli/C/2023/1226/oj/eng.

is to frame the activity of social media platform regarding personal data. The *Digital Services Act*, which will enter in force in its entirety in early 2024[5], provides interesting solutions to these issues the analysis of which will be developed in the third part of the development. However, FIMI is only one example of why personal data should be protected for purposes of national security. This necessity is also enlightened by the, not so old, banning of TikTok from the professional devices of officials pronounced by US and the European Commission (hereinafter: "EC")[6]. Those bans are motivated by the fear that this application is sending personal data to the Chinese offices of Bytedance, to the final benefit of Chinese intelligence services[7]. The actuality of this subject questions in a way, the necessary to protect national security to defend the rights to personal data protection. Hence, questioning the dialectic between personal data protection and national security calls to analyse both the limits the concept can bring to each other, and the way they work together.

In the context of this master's thesis, this dialectic is to be studied in a defined geographical area: the European continent. With respect of the nature of our field, it'll be required to qualify this approach in legal terms. To do so, and under the positivist method, attention will be brought on the sources of law, and the substance of its latter. Hence, it implies to determinate which entities are empowered with the legislative, executive, and jurisdictional functions; even more, to determinate which of them is the more influencing, on the previously mentioned dialectic.

On the geographical criteria, few preliminary developments. Considering a European approach implies that the approach is flowing from European actors, nothing more, nothing less. The question of the territorial, temporal and personal scope of application of this approach is open. Thus, the subject calls to question the content of a trend, of a movement, of a European fashion to apprehend the dialectic of personal data protection and national security. A European approach requests to interrogate the globality, the similarity, of actions undertook by European states on the matter of our subject. It requires to assess whether Europeans states' actions present enough

---

[5] Article 93, 2. DSA

[6] Federal Register. « Protecting Americans' Sensitive Data From Foreign Adversaries », 11 june 2021. https://www.federalregister.gov/documents/2021/06/11/2021-12506/protecting-americans-sensitive-data-from-foreign-adversaries.; European Commission - European Commission. « Commission Strengthens Cybersecurity ». Press release. Consulted on 23 december 2023. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1161.

[7] « Rapport fait au nom de la commission d'enquête (1) sur l'utilisation du réseau social TikTok, son exploitation des données, sa stratégie d'influence », Sénat, consulted on 23 december 2023, https://www.senat.fr/notice-rapport/2022/r22-831-1-notice.html.

similarities to reveal a common trend, an approach. Such possibility, logically, would be the natural result of agreements between European states to act in the same way; in fact, they do so within two international organisations: the Council of Europe, and the EU. The objectives of the Council of Europe are mainly focused of the protection of fundamental rights within the Europe. To that purpose it sits notably, but not exclusively, on a comprehensive code of fundamental rights: The Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter: "ECHR"), the constructive interpretation of which allowed it to become timeproof. On the other hand, the EU is an international organisation to which its Members States (hereinafter: "MS") agreed to transfer competences, and under the authority of which they put themselves in the field of those competences. As both have for purposes the protection of human rights, these organisations are the more relevant to address the dialectic of the subject. Also, they both recognise the competence of the MS to protect their national security, as an inalienable part of their sovereignty. Thus, a part of this master's thesis will conduct a legal analyse of European states' behaviours to protect their national security, more precisely on the limit they find in the reviews of the supranational entities' legal called to ensure personal data protection.

Once these preliminary developments made, let's investigate more deeply the content of that dialectic: the meaning of its constituents.

National security is a very debated notion, for which the need for a common understanding in legal terms is intense. In a way, it can be affirmed that, what was peculiar about the definition of national security, was its lack of definition; for a long-time national security remains on the borders of the Law. It was for States the perfect legal basis to avoid the application of law, to limit fundamental rights, and to adopt extraordinary measures with restricted judicial review, if not at all. Both ECHR and EU orders selected different approaches to apprehend the notion of national security. the ECHR and Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) (hereinafter: "Convention 108), tolerates only limitation "necessary in a democratic society". On the other hand, the EU legal order goes further: while the Charter on the Fundamental Rights of the European Union (hereinafter: "CFREU) tolerates only limitation under article 52§1 regime, secondary law provides both limitation clauses with a regime similar to Article 52§1, and exclusion clauses. Accordingly, to these latter, and with respect of Article 4 Treaty on the European Union (hereinafter: "TEU), because it is a field outside EU law's scope of application, MSs won't be under personal data protection secondary law when there are acting for

purpose of national security. In that view, it is possible to assess that the EU, with respect of article 4 TEU show itself more "respectful" of MS's will of retaining competences in the field of national security. However, a quick of analysis of the cases-law will demonstrate that national security exclusion provisions were interpretated very strictly, to the extent where one can argue that they lost all effectiveness. Practically, this strongly limit, or even eradicate, MSs' range of motion outside the scope of EU personal data protection law.

On the other hand, *Personal data protection* is considered across the European continent as a fundamental right. The Council of Europe is the oldest, with its ECHR made in 1951, far before the conception of the notion of personal data, to protect this right. To do so, personal data protection was interpreted as a component of the right to private life protected by Article 8 ECHR. Moreover, the Council of Europe has a very intense normative activity through the conception of numerous conventions, the number 108 of which is specifically designed to protect personal data. However, Convention 108 doesn't benefit from an enforcement system as strong as ECHR's. Indeed, the ECHR is in last resort controlled by the ECtHR, while the Convention 108 can only be presented before national judges, with no control of its correct application. In that context, the Convention 108 is under the traditional direct effect theory. Under international law legal theory, direct effect will be recognised to a norm if it reunites two criteria: first, the intentions of this norm's creator to directly affect the situation of the individuals, second, the wording of the norm makes it sufficiently clear and complete to not need further implementation acts. In EU law, the intention criterion is presumed[8]. However, in the Council of Europe, only the European Convention for Human Rights benefits from direct applicability, the conventions signed within this Council's framework remains to demonstrate the completion of these two criteria. Hence, Convention 108 is dependent of its Parties transposition, with, to mention it once again, no control of the national measures' adequacy to implement this Convention.

Distinction between processing in General Data Protection Regulation (hereinafter: "GPDR')'s meaning compared to intelligence services meaning is another relevant question of today. The need for a concept definition also applies within the processing undertaken for national security in

[8] On that subject, see: P. Pescatore, 2015, "The doctrine of "direct effect": an infant disease of Community Law", E.L. Rev. 2015, 40(2), 40(2), 135-153

matter of intelligence. Indeed, while in the GDPR every action on the data is a processing and, therefore, an infringement of Article 8 CFREU, surveillance vocabulary uses the word processing only to refer to the analysis of the data once collected[9]. The action of collecting the data would then be referred to by using the word interception. This master's thesis will use GDPR's meaning to apprehend broadly every action on data, as the definition of GDPR was intended to do.

The review undertook by the Council of Europe and the EU, which will be the subject of the beginning of the following developments, is of a judicial nature. It must be mentioned that it is not only the review of these entities, as being authorities able to sanction the infringement of a legal requirements, that constitute the entirety of this legal systems' control. Indeed, within these two systems, the supreme control of the supranational courts is complemented by the national judges' control, which are the first entitled to sanction the infringement of this law. The importance of the "dialogue between judges" in the conception of a two head European approach is another relevant aspect. The subject of this master thesis mention "European approach", which is to suggest that there is one and only European approach. Such unicity among two different legal orders could surprise one not familiar to the intertwining of those two courts. Indeed, if those two entities share values, principles, and their members, they remain distinct and institute two different legal orders claiming autonomy, the EU especially fiercely through the interpretation of its court. Hence, the presentation of that cooperation is a necessity for the following development. On paper, Article 52§3 provides for an obligation to the CJEU of conform interpretation of CFREU rights to the one protected by the ECHR. Further, we can see in both courts case-law numerous references to each other's case law, which leads author to recognize a *dialogue des juges*. This dialogue more generally participates, to some extent, to harmonise the level of protection amongst those two orders. The materiality of this unicity will be the object of further discussion, to mention notably that, if the two orders are somehow largely coordinated to recognize the overarching importance of fundamental rights, they diverge on the final balance of interest.

Research problem: This master's thesis seeks to answer the following question: "How fundamental right to personal data protection's enforcements by two supranational legal orders restrict States'

[9] Véron, Noémie. « Protection des données personnelles et renseignement: contribution à l'identification d'un régime juridique autonome ». Pau, 2022.

margin of appreciation to defend their national security in a fashion that can be qualified of European approach?"

Relevance of the final thesis: this master's thesis finds its relevance in its answer to the question to know whether there is a European approach to dialectic between personal data protection and national security. This question is made important today by the two points, personal data need to be protected both from imperatives of national security, and for imperatives of national security. In the first situation, the situation is that the means used by institutions to protect national security are more infringing right to personal data, for example by the possibility of mass surveillance. One the other hand, suspicions of foreign influence, or processing personal data for purposes of manipulating elections' results is a raising concern among democratic societies, which call for new legislation. These two situations illustrate the necessity today to answer the question mentioned before. It is a contemporary necessity because States are always under the "tentation" to put in place always more invasive legislation to ensure their security, for example in France for the incoming Olympic games. On the second situation mentioned, it's a contemporary necessity because early 2024, EU legislation will enter in force posing brand new framework on the digital area, putting a term to what could have been called before a framework. Hence, it that matter, this master's thesis is located at a crossroad where solution from the past, inherited from case-law will be put to a stress test (the Olympic games in France for example), and where ongoing concerns are now stopped by new legislations, the efficiency of which can be already assessed by a careful analysis of the provisions.

Sources used in the thesis: For this work, relevant cases-law of the ECtHR and CJEU were systematically analysed. To find to relevant cases in the CJEU's database the keywords "national security" and "personal data" were used. In the ECtHR's database, research was performed by using the keyword: "personal data" and the criterion "art. (8-2) National security". Based on the case-law founds, the relevant legal acts, and other linked cases-law were found. Hence, in the ECtHR, the ECHR was studied, and the CJEU called to the analyse of the treaties, of the CFREU, and of several secondary acts. However, other legal act was found in a more direct manner. In Council of Europe order, the Convention 108 was to be studied, and within EU law, DSA regulation, as it was adopted recently, was to be studied as well.

To find scholars literature on the subject, the same keywords "personal data" and "national security" were used in MRU's and in Bordeaux University's databases. For the first part, general literature on European Law[10] was used, the main input for the second part was the doctoral thesis of Olivia VERON[11], while the third part was essentially done through autonomous analysis of the legislation.

Scientific novelty: The novelty of this research is to present comprehensively how national security can be defended both trough limitation and increased protection of personal data. To do so, this master's thesis will present how intertwined are the CJEU and ECtHR to control the limitation to that right and how the EU is the privileged entity to initiate a European approach protecting personal data subjects for purpose of national security.

Significance of research: This research's significance is to bring foundations to the understanding of how personal data protection and the concept of national security interact within the European continent. This is made important by the constant need for data protection since the technologies to process have evolved in ways that limit always strongly this right. This study aims to allow for a better understanding of the obligations made to the state, of the action taken by the EU to protect personal data in conjunction with national security. It also seeks to identify gaps where scholars could investigate, or for the institutions to act on.

The aim of the research is to disclose how the protection of the fundamental right to personal data enforced by two supranational legal orders restricts States' margin of appreciation to defend their national security in a fashion that can be qualified of European approach.

To do so, the *objectives of this research* are the following:

1. To demonstrate that, national security remaining with States' competence, they are the only one entitled to act for this purpose directly. When they intend to do so, they are limited by

[10] For example, Picod, Fabrice, Cécilia Rizcallah, et Sébastien Van Drooghenbroeck. Charte des droits fondamentaux de l'Union Européenne: commentaire article par article. 3e éd. Collection Droit de l'Union européenne 2. Bruxelles: Bruylant, 2023 ; Tinière, Romain, Claire Vial, et Frédéric Sudre. Droit de l'Union européenne des droits fondamentaux. Collection Droit de l'Union européenne 16. Bruxelles: Bruylant, 2023 ; Morano-Foadi, Sonia, et Lucy Vickers, éd. Fundamental rights in the EU: a matter for two courts. Modern studies in European law. Oxford ; Portland, Oregon: Hart Publishing, 2015.

[11] Véron, Noémie. « Protection des données personnelles et renseignement: contribution à l'identification d'un régime juridique autonome ». Pau, 2022.

the duty to respect fundamental rights As the ECHR and the CJEU are the competent authorities to defend the right to personal data protection, the analysis of their case law will enlighten the regime applicable to MSs' action to protect national security, confronted to the imperative to protect data subject. Hence the first objective of this research is to demonstrate the first side of the European approach is created by the praetorian control of European States' actions to defend national security.

2. The fact that States are the only one entitled to protect their national security doesn't mean that an entity adopting a measure indirectly participating to protect such security is necessarily acting outside the scope of its competences. Indeed, by protecting protect personal data, or by adopting measures "which have as their object the establishment and functioning of the internal market"[12], EU institutions can participate to enhance the national security of its MS. The analysis of EU institutions' participation to protect the security of the MS is the second objective of this master's thesis.

3. The third objective is to analyse, within the two-objective presented, the relationships between the different actors involved, in addressing the dialectic of our subject.

The statement(s) to be defended: there is no common European approach to the direct protection of national security because of the necessity to protect personal data. However, there is a certain degree of coherence between the limitations established by ECtHR and CJEU in their case law. Hence their case-laws, to a limited extent, design a European approach to the legislative framework the European states can adopt to protect national security, without infringing the right to personal data. As we know, the two courts have different materials to interpret. Hence, one could think that there is no European approach to the limitation of the aforementioned margin of appreciation. However, because the two courts make frequent reference to each other in their case law, and because the CJEU is notably under the obligation to be in adequation with ECtHR's level of protection, it is possible to affirm that there is a certain degree of coherence between the limitation provided for by the two courts' case law, which can be qualified as one side of the European

[12] Article 114 TFEU

approach we will present during this work. It is mainly constituted of requirements made to the States in the definition of their legislation limiting personal data protection, to ensure that a control of proportionality is made, and renewed, from the beginning to the end of the limitation. It's what is called an "end-to-end" means of protection.

The EU, because of its attributed competence, and the subsequent executive and legislative powers, can initiate a European approach. Despite having no competence in national security, the EU can indirectly protect it by acting in one of its attributed competencies, here personal data protection[13].

Hence, if both of these phenomena can be qualified as European, the first one consisting of restricting European States' discretion in defending their national security, and the second being the EU's ability to initiate legislative trends protecting the security of its MS through the accomplishment of treaties' objectives, the second is more restricted in terms of participants. If the first one can be qualified as reactive, its design being drawn a posteriori through judicial review, the second is made a priori, as being of a legislative nature. The conjunction of those two constitutes the European approach to personal data protection and national security.

Research methods: To perform this research, the first part conducted a systematic analysis of ECtHR and CJEU's case law to note their main characteristics and tendencies. It was then compared to legal literature to determine whether the judges' inclinations in this matter were consistent with what was thought of as being their traditional control. Finally, the two case laws were compared to give an opinion on the level of protection they offer. Lastly, the third part used an exegetic method to enlighten the rules considered as having the most potential to address the issue of foreign influence.

The structure of the thesis:

To answer the question identified within the problem research, a three-part demonstration will be led. The first and second parts will demonstrate the first side of the European approach, which is the protection of personal data against limitations taken for purposes of protecting national

[13] Article 16 TFEU

security. Respectively, they will present the supranational orders defending the right to personal data protection: the Council of Europe and the EU, their respective materials, and mechanisms of enforcement. The third part, the last, on the other side of the European approach, will demonstrate how the protection of personal data can contribute to national security protection through the case study of the framework for the processing of personal data by online service providers.

Limitations: This master's thesis presents the following limitations. First, when assessing the influence of the Council of Europe on what was to be determined as the European approach, the Convention 108's effect had to be stepped aside. Indeed, as presented before, this Convention, and the opposite of the other legal instruments mentioned and studied within this thesis, doesn't benefit from the control of a supranational court to ensure the coherence of its application. Hence, understanding the efficiency of this Convention is dependent on a comparative analysis of its application and enforcement within national orders, which is outside the scope of this research.

Second, the secret nature of the measure undertaken to ensure national security limits the analysis of national receptions of the regime drawn by supranational courts. Thus, this master's thesis first part is dedicated to the framing of States' margin of appreciation, and the study of this framework only. Indeed, the study of such reception within European States' legal order would call once again to a comparative analysis, which goes beyond the scope of this research.

Thrice, this study had difficulties finding normative documents providing for the prohibition of TikTok coming from the EU institutions or a state from which the official language is understood by the author. Hence, the analysis of TikTok prohibition on EU of French officials' devices is strongly limited.

Lastly, this study didn't seek to perform a comparative analysis between the protection offered to data subjects on the European Continent and the one offered by other countries, such as the US, which is known to have a different stance on that matter. Indeed, for such a study, it'd be necessary to have a clear and comprehensive understanding of the regime applicable in Europe, which is what this master's thesis aims to contribute to.

1. THE PROTECTION OF PERSONAL DATA OVER THE EUROPEAN CONTINENT, A COHABITATION BETWEEN TWO LEGAL ORDERS

The present section will present and distinguish the scope of application of these legal orders, to find where they overlap and where they complement themselves, and how they protect the individuals from infringement of their rights from MSs and EU institutions. This choice is justified by the fact that national security remains within European States' competencies, and because, to identify the European Approach, it is necessary to look for the tool generally affecting all, or the majority, of European States.

Therefore, both subchapters will firstly present the relevant law applicable to personal data protection in the two orders, and will, secondly, present their enforcement mechanism. The first one is dedicated to the Council of Europe and the second to the EU.

1.1. The Council of Europe, two normative tools with different control mechanism

The Council of Europe protects personal data protection through two main instruments, the ECHR, and the Convention 108. The presentation of these two tools will be the subject of a first part while a second will be dedicated to the study of ECtHR mechanism of enforcement.

1.1.1. Article 8 ECHR and Convention 108 to 108+, an inclusive approach

The objectives of the Council of Europe are mainly focused of the protection of the fundamental rights within the Europe. To that purpose it mainly sits on a comprehensive code of fundamental rights: the ECHR. Even though having been designed in 1951, a constructive interpretation allowed this instrument to be timeproof and to answer the evolving problematics of societies.

Related to our subject is its Article 8, providing for a *Right to respect for private and family life* which evolutive interpretation allowed to comprehend problematics relatives to the protection of personal data. The article postulates for the possibility of limitation, as long as this latter is

provided for by national law and "is necessary in a democratic society"[14]. This concept of necessity in a democratic of society is further detailed by this master thesis as including "*interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or moral, or for the protection of the rights and freedoms of others*". If, in normal conditions personal data protection, as the other rights protected by the ECHR, involves for the contracting parties both negative and positive obligations, in matter of national security, the Court tolerates that the parties are exempted, for example, to notification of infringement within the data, or access to data within a reasonable time. This is justified as such obligation could hinder the effectivity of measures needing secrecy for their effectivity to be ensured[15].

Alongside this general provision, applicable to all the members to the ECHR, is the Convention 108 exists, a forerunner in matter of personal data protection. The opening of this convention to the signature of extra-European countries contributes to an exportation of the European approach. Indeed, in addition to the 46 members of the Council of Europe, 9 states outside the European continent signed Convention 108[16].

However, Convention 108 found natural limits coming from the fact that it has to be applied by national judge, without the control of a supranational court having interpretative monopoly, or powers to address sanction, when discrepancy in the application is constated. Hence, individuals must claim before their national judge violation of this international convention, which has primacy over national law under classic international law. However, its degree of *justiciability* depends on whether the claimed provision has direct effect.

For a norm to be directly used by an individual, it must be "self-executing"[17]. As presented before, this requirements in international public law requires from a provision to meet two criteria, one subjective, the other objective. Some[18] affirms that Convention 108 is limited within national

[14] Article 8(2) ECHR
[15] (Guide to the Case-Law of the of the European Court of Human Rights Data protection Updated on 28 February 2023, §79).
[16] Treaty Office. « Full List - Treaty Office - Www.Coe.Int ». Consulted on 23 december 2023. https://www.coe.int/en/web/conventions/full-list.
[17] Dupuy, Pierre-Marie, and Yann Kerbrat. 2022. « Droit International Public ». 16e. ed. Précis. (France). p470-471
[18] Walter, Jean-Philippe. « La Convention 108, un complément nécessaire à l'article 8 de la CEDH à l'heure du numérique ». Civitas Europa 49, no 2 (2022): 251-61. https://doi.org/10.3917/civit.049.0253. P256-257

judicial order due to the wordings of its article 4(1): "Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter". However, the author suggests another view. Indeed, it seems that article 4 is nothing more than a generic provision calling States to apply the content of the said agreement, followingly the *Pacta sunt servanda* rule, and doesn't rule out the possibility for the individuals to call out the application of the agreement. Indeed, as the wording of other articles of this Convention seem to comply with the criteria of precision, it would be the subjective of criteria that can, arguably, discard this Convention's provision to be self-executing.

To sum up, it is possible to affirm that, within the Council of Europe, two tools serve to protect personal data: Article 8 ECHR and Convention 108. However, this last, to the contrary of ECHR, doesn't benefit from a supranational court to be enforced. Hence, the question of its effectivity would require for it to be solved a comparative analysis of national legal orders, which is outside the scope of this research. The following part will thus develop the enforcement mechanism of the EHCR.

1.1.2. Exhaustions of domestic's remedies, and authority of ECtHR's decision

The rules governing the two contentious proceedings of the ECtHR are provided in Articles 33, 34 et 35. While Article 33 provides for an interstate proceedings, the following analysis will present Article 34 and 35. Indeed, the kind of proceeding provided by Article 33 is rarely used by States parties to the ECtHR which are unwilling to use it for the politic message it sends.

Meanwhile, ECtHR's admissibility conditions and personal affectation requirements provided by Articles 34 and 35 are key to understand to what extent is restricted individuals' access to Strasbourg's judges. Among the admissibility conditions provided for by Article 35, the main hurdle to the individual action, which must be based on personal interest, is the requirement of domestic's remedies exhaustion. Indeed, among other requirements, the Court requires from the individuals for their action to be receivable, to present only after having exhausted all useful

remedies available in their domestic orders[19]. In the matter of national security and personal data, where secrecy found a privileged place, this requirement was very early the source of difficulties. Indeed, it's hard for an individual to demonstrate that he was personally affected by a national surveillance scheme when he can't demonstrate the practical implication of such a scheme. Indeed, and it is a *leitmotiv* of this subject, the secrecy of national security measures is a strong impediment to *in concreto* analysis, to concrete litigation[20]. Indeed, the secrecy of the measures adopted means the concerned individual won't systematically be able to demonstrate his personal affectation to meet Article 35's requirement of admissibility. This issue was to be solved very early by the ECtHR which allowed for an individual to bring an action against a legislation *in abstracto,* under some requirements. Historically, this extension finds deep roots in the ECtHR's case law. As mentioned before, it as soon as in 1978[21] that the Court admitted in *Klass and others v. Germany* the possibility to diverge from the requirement of personal affectation in case involving secret surveillance. However, condition for this extension "were to be determined in each case according to the Convention right or rights alleged to have been infringed, the secret character of the measures objected to, and the connection between the applicant and those measures"[22]. It is in the Kennedy[23] and Zakharov[24] cases law that the Court clarified once all the divergent interpretation on whether this requirement should be discarded. To assess whether an individual should be able to contest a national law *in abstracto* before the ECtHR, the Court decided to take a two-step approach. Firstly, the Court assess the scope of the national legislation to determine whether "the applicant can possibly be affected by it, either because he belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his communications intercepted"[25]. Secondly, the Court examine the available national remedies, and their effectiveness, to determine whether the applicant has a chance to contest the national legislation within his national

[19] De Jong, Baljet and Van Den Brink v. the Netherlands, No. 57466/13, 60013/13, 64648/13, 75690/13, 78942/13 (ECtHR 22 mai 1984), par.39
[20] Véron, Noémie. « Protection des données personnelles et renseignement: contribution à l'identification d'un régime juridique autonome ». Pau, 2022.
[21] Klass and Others v. Germany, No. 38581/16, 41914/16, 57510/16, 62644/16, 7190/17, 10973/17, 12530/17, 19411/17, 22087/17, 28475/17, 78165/17 (ECtHR 6 septembre 1978)
[22] Klass and Others v. Germany, No. 38581/16, 41914/16, 57510/16, 62644/16, 7190/17, 10973/17, 12530/17, 19411/17, 22087/17, 28475/17, 78165/17 (ECtHR 6 september 1978) p34
[23] Kennedy v. the United Kingdom, No. 26839/05 (ECtHR 18 may 2010), par. 122/123
[24] Roman Zakharov v. Russia, No. 47143/06 (ECtHR [GC] 4 décembre 2015).
[25] Roman Zakharov v. Russia, No. 47143/06 (ECtHR [GC] 4 décembre 2015), par. 171

jurisdictional order. The Court, however, precise that the second criteria is the most important. It states that, in the absence of effective remedies at the national level, a possible affection under the first criteria isn't needed to demonstrate while, if there are national remedies, the applicant must demonstrate that s/he belongs to a special category of individuals "potentially at risk of being subjected to such measures"[26].

Extraterritoriality of the ECHR is another important feature to mention as it'll be, to some extent, a factor of the European approach's exportation. The question of how the decisions of the ECtHR can have extraterritorial effect is raised by the wording of Article 1 ECHR: "The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention.". Here the key to comprehension flows from the fact the obligation for the contracting parties to secure ECHR's rights and freedoms applies to everyone "within their jurisdiction". The notion of "jurisdiction" requires no attention to whether the individual has the citizenship or is located on the territory of the contracting party, what only matters is the effective control that may have on the *legal situation* of the individual[27], even if this control happened to be on an individual located over the territories of a foreign country[28]. In matter of personal data, the Court hence sanction the "virtual control"[29] that one contracting party may have on an individual. The virtuality of the matter makes easy for a state to affect legal situation of an individual outside its border. However, the analysis of ECtHR's case law doesn't reveal that this issue was addressed substantially. Indeed, in *Big Brothers Watch,* the Court merely recognised that the jurisdictional competence of the UK was to be recognised[30], in the absence of objection of the government on that matter. Moreover, the recognition of a *ratione personae* competence to individual outside the traditional wasn't raised in *Centrum for Rattvisa* case-law neither[31]. However, this is surprising as the question of *ratione personae* should be raised by the Court of its own motion[32]: "Although the respondent State did not raise any objection as to the Court's competence ratione personae, this

[26] Roman Zakharov v. Russia, No. 47143/06 (ECtHR [GC] 4 décembre 2015), par.171.
[27] Bignami, Francesca, et Giorgio Resta. 2018. « Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance », s. d. p16
[28] « Practical Guide on Admissibility Criteria », ECHR-KS, version of 28/02/23
[29] Bignami, Francesca, et Giorgio Resta. 2018. « Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance », s. d. p17
[30] Big Brother Watch and Others v. the United Kingdom, No. 58170/13, 62322/14, 24960/15 (ECtHR [GC] 25 mai 2021, par.272
[31] Centrum För Rättvisa v. Sweden, No. 35252/08 (ECtHR [GC] 25 may 2021
[32] Practical Guide on Admissibility Criteria Updated on 28 February 2023, §271 and cases-law cited).

issue calls for consideration ex officio by the Court"[33]. Such diligence, beyond the sake of a solid demonstration, is made even more necessary since UK Investigatory Powers Tribunal held an opposed stance in 2016 and claimed that "a contracting state owes no obligation under Art. 8 to persons both of whom are situated outside its territory in respect of electronic communications between them which pass through that state"[34].

Moreover, the effectiveness of ECtHR's decision is restricted by the modality of its control. Indeed, ECtHR proceeds in principle within the limits of an *in concreto* analysis, by appreciating domestic laws as facts. Due to that, the ECtHR has no jurisdiction to directly address the legislation of one of its contracting parties, to indicate where the problem lies specifically. Hence, even after an ECtHR ruling on an infringement, nothing binds the States to adopt a corrected legislation, and new proceedings can emerge from an issue on which the ECtHR has already ruled. This limit to ECtHR's decision efficiency can be mitigated by two successive point, one general, the second much more specific. First, despite being indirect, the control of the domestic legislation is far from being a "stopgap". Indeed, due to the phenomenon of redundant cases, meaning proceedings born from as systematic issue of a contracting party's legal order, ECtHR intensified its review to the point that some depicted it as being "highly intrusive"[35], of a "constitutional character"[36]. Second, and precisely related to our subject, in matter of mass surveillance the ECtHR sometimes adopts an *in abstracto* control of the domestic legislation.

Two more remarks can mitigate the idea that the ECtHR is impotent to address mass litigation. First, the Court has developed the practice of pilot-judgement procedure. Now codified within article 61-1 of the Court Statute, this procedure first saw the light of day in *Broniowski v. Pologne*[37]. It allows the Court to deliver a more efficient decision to repetitive cases, through the incrementation of its decision with provisions related to the systematic problem raised by the domestic legislation, and to the possibilities for improvement. Second, with the entry in force of

---

[33] Sejdić and Finci v. Bosnia and Herzegovina [GC], 2009, § 27

[34] Bignami, Francesca, et Giorgio Resta. 2018, « Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance », s. d. p17, and sources referred to: Human Rights Watch Inc. v. The Secretary of State for the Foreign and Commonwealth Office, [2016] UKIPTrib 15_165-CH [60]

[35] Wolfang Weiss in "Fundamental Rights in the EU - A matter for two courts"; Sonia MORAN-FOADI & Lucy VICKERS; Bloomsbury; 2017; p72

[36] Wolfang Weiss in "Fundamental Rights in the EU - A matter for two courts"; Sonia MORAN-FOADI & Lucy VICKERS; Bloomsbury; 2017, p72 and related citation

[37] Broniowski v. Poland, No. 16153/09 (ECtHR [GC] 22 juin 2004).

Protocol 16[38], the ECHR, to solve a domestic litigation, and since August 1st, 2018, can be referred by the member states' highest courts a question upon the interpretation and application of the ECHR. However, ECHR's decisions efficiency is limited by the lack of means of sanction available to the Court, or to Council of Europe's assembly. To the difference of the CJEU, no pecuniary sanction, or whatsoever, which could lead to enforce ECHR's decisions, this latter having mainly a declarative authority[39]. To this day, no referral has been made to the ECHR on the basis of Protocol 16, nor has the Article 61-1 used in our subject. This might give the clue that States concerned by the cases have taken the necessary measures to resorb the infringement, or simply that no other individuals sought the judgement of the ECtHR. However, the analysis of the reception by the States of the cases-law involving personal data protection and national security is outside the scope of this research, even thought it would be interesting to assess to what extent ECtHR' decisions had practical consequences on national legislations.

The precedent developments sought to demonstrate that the main tool to protect personal data within Council of Europe's legal order is the ECHR. Indeed, this Convention is more effective to protect data subject than the Convention 108, even though it is more precise, because of the unified control of its application led by the ECtHR on the ECHR. If by design, the ECtHR, and more generally the Council of Europe, carried flaws within its enforcement mechanism, the input of protocol 16 or of the pilot-judgement procedure increased its efficiency. As mentioned before, a part of the States parties to the Council of Europe are also members of the EU, which also defend the right to persona data protection, which make these last under the authority of two supranational courts. The following part will address the situation of these States, to present to what obligations they subject to, and under which system of enforcement they have to act.

1.2. The law of the EU, a more precise tool with variable geometry scope of application

EU law has a peculiar, to not say complex, scope of application. The EU has a restricted number of members, and, logically, EU law on personal data protection can only be applied where EU law

[38] Protocol No. 16 to the Convention on the Protection of Human Rights and Fundamental Freedoms Strasbourg, 2.X.2013 ; https://www.echr.coe.int/documents/d/echr/protocol_16_eng
[39] Gauthier, Catherine, Sébastien Platon, et David Szymczak. Droit européen des droits de l'homme. ve

is applicable. As simple it may sound, it is in fact much more complex as the CJEU has developed an extensive interpretation of what is the "general" scope of application of EU law. Even more, the intertwining between the relevant EU secondary legislations isn't exempt of difficulty neither to determine the applicable law. Overall, in primary law, the competence of the EU extends wherever the authors of its funding treaties, in accordance with the principle of conferral, choose to give powers to the institutions. However, the CJEU developed the theory of implicit competences with the affectation doctrine[40] and the necessity doctrine[41]. This subsection will firstly present the reasoning around the scope of application of EU law, whether it is its primary law or the layout of secondary legislation. Secondly, it will develop the EU legality control's modalities.

1.2.1. Application of EU law, the *shadow* of the Charter and the entanglement of secondary legislations

The EU acts upon conferral principal. It finds a competence in matter of personal data protection in Article 16 TFEU, which provides for the competence to "lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data" under the ordinary legislative procedure. Hence, MS acting under the Council of the EU (hereinafter: "the Council"), and the EP co-exercise the legislative power, with the right, sometimes obligation, for the EC to initiate the legislative procedure by a proposal.

Next to this general legal basis, article 39 TEU provides, within the CFSP chapter, a special legal basis for the protection of personal data. This legal basis however never found use; it's therefore possible to affirm that MS own a certain margin of manoeuvre in matter of personal data protection when it comes to external relations. Article 16 TFEU on another hand, had had a prolific usage

[40] Procureur du Roi v Benoît and Gustave Dassonville, No. Case 8-74 (ECJ 11 July 1974).
[41] Opinion given on the Draft Agreement establishing a European laying-up fund for inland waterway vessels, Opinion 1/76 (ECJ, 26 April 1977).

over the time. Its use led to the edification of a comprehensive, and complex, legislation architecture.

The EU secondary legislation on personal data protection is characterised by its entanglement. Leading the way is the GDPR officiating as the *lex generalis* of EU personal data protection. The GDPR is flanked by several legislates tools, playing the part of *lex specialis*: E-privacy directive[42], Law Enforcement Directive[43], EU institution regulation[44]. Overarching this construction is the article 8 CFREU, which, presented the novelty of elevating as a fundamental right the protection of personal data.

The EU law, even more than the ECHR, as described before, develops its effects across its border and can be seen as an exporter of norms. One of the channels for the EU to export its norms is through its commercial power. For example, third states companies wishing to enter EU market must meet standards for the goods or services exported[45]. For example, the GAFAM wishing to provide service on the European market will have to comply with the GDPR to do so. In matter of personal data protection, this extraterritoriality is even more fundamental that EU citizen's data are widely use across the world. Hence, the EU, through the action of its institutions, the negotiating power of the EC, as well as the control of legality of the CJEU, ensure a "bimotored" protection of the personal data across the world[46]. Article 45 GDPR provides that, for an easy transfer of data from the EU to a third state country, the receiving country should offer an equivalent protection to the data than EU law delivers. With that regulation, third state wishing to

---

[42] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 201 OJ L § (2002). http://data.europa.eu/eli/dir/2002/58/oj/eng.

[43] Directive (EU) 2016/680 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 prosecution 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, 119 OJ L § (2016). http://data.europa.eu/eli/dir/2016/680/oj/eng.

[44] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.), 295 OJ L § (2018). http://data.europa.eu/eli/reg/2018/1725/oj/eng.

[45] Dimitrova, Anna, et Maja Brkan. « Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts before and after the NSA Affair ». Journal of Common Market Studies 56, nº 4 (mai 2018): 751-67. https://doi.org/10.1111/jcms.12634. p.755

[46] Brkan, Maja. « The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors ». Maastricht Journal of European and Comparative Law 23, nº 5 (2016): 812-41. p.837

ensure optimal business condition to their companies requiring data from the EU, are strongly encouraged to develop a solid data protection legislation. For some countries, as the USA, it's especially necessary since the GAFAM are American companies.

The quality of the protection provided by third states is then sanctioned by the EC through an adequation decision[47]. However, once granted this adequation decision isn't permanent. As being a part of the secondary legislation, this decision's legality can be challenged directly or indirectly, throughout times. Hence, with evolution of technology, or circumstances, this decision, either by an initiative from the EC, or following an annulment decision from the CJEU, can be withdraw. It was the case for the *Safe Harbor* agreement between the EU and the USA, the illegality of which cause the adequation decision on which it was based to be withdrawn. Indeed, in Grand Chamber, the CJEU, in the decision *Maximillian Schrems v Data Protection Commissioner*[48], invalidated the adequacy decision adopted by the EC or the lack of proportionality of the limitations to personal data protection of the USA's legislation. This case put the emphasis for the need of a new transatlantic agreement in reaction to Snowden's revelation[49].

More generally, the Charter also finds an extra-territorial application. Indeed, as being the "shadow" of EU law[50], the Charter must be applied wherever EU law is applied as provided by the Court in *Åklagaren v Hans Åkerberg Fransson*: "The applicability of European Union law entails applicability of the fundamental rights guaranteed by the Charter"[51]. Hence, when, for example, the GDPR finds to be applied in a third countries, or when a bilateral agreement of EU is applied, the Charter is relevant to the interpretation of such agreement by the third states judges[52]. The second channel of EU law exportations is material, through the regulation of PNR transfers. In that matter where EU has specific secondary legislation in force, the EU influence other member states through the negotiation of international agreements. Under the review of

[47] Article 45 GDPR
[48] Maximillian Schrems v Data Protection Commissioner, No. Case C-362/14 (ECJ 6 octobre 2015).
[49] Dimitrova, Anna, et Maja Brkan. « Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts before and after the NSA Affair ». Journal of Common Market Studies 56, nº 4 (mai 2018): 751-67. https://doi.org/10.1111/jcms.12634. P764
[50] Koen Lenaerts, President of the Court, keynote speech at the conference 'Making the Charter of Fundamental Rights a reality for all' ('Charter event'): https://ec.europa.eu/info/events/2019-conference-eucharter-fundamental-rights-2019-nov-12_en
[51] Åklagaren v Hans Åkerberg Fransson, No. Case C-617/10 (ECJ 26 février 2013). §21
[52] Brkan, Maja. « The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors ». Maastricht Journal of European and Comparative Law 23, nº 5 (2016): 812-41. p.831

CJEU, those can't be in violation of EU protection of personal data. Opinion 1/15[53]related to EU-Canada is the most recent example of EU scrutiny over this kind of agreement.

As it has been demonstrated, the borders of EU law application remain uncertain due to the extension of EU competence through the implicit power doctrine. It allows for the EU institutions to act in new fields, and, subsequently, for secondary legislations to apply, notably through its extraterritoriality. Hence, knowing now when EU law is applied, to understand its content, we firstly have to understand the way it is interpretated to discover in the second chapter its content. Indeed, the method of its enforcement influence its content.

1.2.2. The legality control within the EU legal order

The overarching distinction of this part is to be made between the control of legality of MS's acts in one hand, and the legality of EU's acts in another hand. What reunites these two is the share responsibility of national judges to be the common judges of EU law.[54]

The early enforcement of EU law is allowed by preliminary ruling mechanism[55]. The advantage of EU legal system is the fact that a violation of EU law can be invoked as soon as before the first instances judges of a national legal order. Indeed, these latter are, due to the nature of EU law, the common judges of EU law. It is their responsibility to ensure the direct effect and primacy of EU law, with the possibility, if necessary, to discard the application of a national legislation that would be in contradiction with EU law[56]. To help them in that task, and to the final purpose to ensure the uniformity of EU law, the preliminary ruling mechanism allows — as a faculty of the national judge, but as an obligation if he officiates as the judge of last resort[57] — for the CJEU to precise the meaning of EU law, and to indirectly control the conformity of the national legislation, as well to review the legality of EU legislation. Indeed, the Court only use a trickery in the wordings to

[53] Opinion of the Court (Grand Chamber) of 26 July 2017. Opinion pursuant to Article 218(11) TFEU. Case Opinion 1/15. (ECJ 2015).
[54] NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration, No. Case 26-62 (ECJ 5 février 1963).
[55] Article 267 TFEU
[56] Amministrazione delle Finanze dello Stato v Simmenthal SpA, No. Case 106/77 (ECJ 9 mars 1978).
[57] Srl CILFIT and Lanificio di Gavardo SpA v Ministry of Health, No. Case 283/81 (ECJ 6 octobre 1982).

dissimulate the control on MS's acts: EU law "must be interpreted as precluding legislative measures"[58] such as the one that gave birth to the litigation. This proven system allows in theory for a much early control of the supra national court, and in fine, a much early application of the correct rule. In the matter of our subject, the *Quadrature du Net*[59] and *Digital Rights Ireland*[60] cases give examples of preliminary ruling procedure for, respectively, national legislation's indirect review and EU legislation's review.

The control of MS's action legality is completed by the infringement proceedings. This proceeding led by the EC, allow for the EU to sanction formally a MS to invite it to adopt change in its behaviour. To this day, and in the matter of our subject, no judgment has been given.

Lastly, the annulment proceeding complete the scheme of the legality control within the EU. Its aim is the review EU's institutions acts. However, this proceeding is open principally to EU institutions and MS, while individuals must justify an interest in the action, the conditions of which making quite hard for an individual who is not the recipient of an act to obtain access to Luxembourg's Court. A 2006 case *EP v Council of the EU and EC*[61] gives an example in the matter of our subject of such proceedings.

[58] GD v The Commissioner of the Garda Síochána and Others, No. Case C-140/20 (ECJ 5 avril 2022), §129.
[59] La Quadrature du Net and Others v Premier ministre and Others, No. Joined Cases C-511/18, C-512/18, C-520/18 (ECJ 6 octobre 2020).
[60] Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, No. Joined Cases C-293/12 and C-594/12 (ECJ 8 avril 2014).
[61] European Parliament v Council of the European Union (C-317/04) and Commission of the European Communities (C-318/04), No. Joined cases C-317/04 and C-318/04 (ECJ 30 mai 2006).

1.3. Summary

To conclude this part, the first paragraph will compare the different sets of norms provided by these two legal orders to protect personal data, and the second paragraph will compare the systems of enforcement of those rules.

The Council of Europe defends human rights by design. In the matter of personal data protection, two tools: article 8 ECHR, and Convention 108. ECHR benefits from the ECtHR to be enforced and to be interpreted uniformly while the Convention 108 relies on its implementation and enforcement from the national legal orders. Moreover, the question of its reception within legal orders remains. On the other hand, the EU was founded with an economic purpose, and the protection of human rights came later. In the matter of personal data protection, the CFREU offers overarching protection with its Article 8 and is helped by quantities of secondary legislation based on Article 16 TFEU, the GDPR is the *lex generalis*.

The ECHR is enforced by the ECtHR. This court pronounces decisions that have only a declarative authority. The absence of executive force, which can fail to address systemic issues, is tempered by Article 61-1 which provides for the pilot-judgement procedures. However, this procedure never has been used in the matter of our subject, so either States that were involved in a case before the ECtHR changed their legislation or no individuals sought redress after the decision where given. The ECtHR, in reaction to the secrecy that characterizes national security measures, had to bend its conception of personal affectation, to allow for individuals to contest in abstract the legislation allowing for secrecy measures to be adopted. On the other hand, EU law is enforced with time-proven two-stage mechanics. Widely open to EU citizens is the preliminary ruling procedure, which allows for these last to contest either national legislation in an indirect way or the EU law directly. This system is completed by a second stage, before the CJEU directly, with the infringement proceedings to sanction MS that doesn't comply with EU law and annulment proceedings against EU secondary law. It can be affirmed that the EU allows for a stronger system of enforcement of its law against national measures for two reasons: firstly, the preliminary ruling procedure, if it has an equivalent within the ECtHR with Protocol 16, is much more used within the EU legal order. Indeed, national judges, with this mechanism found a privileged place to help

to ensure the uniformity of EU law application. Even more, they are bound to refer to the CJEU if they are judges of last instances, under CILFIT[62] conditions, which largely ensure that questions of EU law interpretation are solved. To sum up, it's the large use, partially as a being a mandatory referring, that allows for the EU preliminary ruling procedure to be more effective than protocol 16. Moreover, while ECtHR usually addresses national measures *in concreto*, with the notable exception of our subject, it remains that its decision only has a declarative authority. On the other hand, in the context of the infringement procedure MS are in the end bound to participate in the procedure, and to comply with the CJEU decision as financial sanction can be addressed. To sum up, it is the lack of sanction addressed by the Council of Europe, or the ECtHR, in case of infringement of the ECHR, that makes the EU law enforcement more effective against national measures.

As some European States are both under the ECtHR and CJEU's control, one could be concerned by the possibility that the relevant States may be under contradictory requirements from these courts. This risk of conflict of system is mitigated, first, the CJEU is under the obligation to give an equivalent level of protection to the rights contained in the Charter that also find to be protected by the ECHR.

Hence, the Second part will analyse more deeply the case law of both courts to determine whether the cooperation tools just mentioned led to the adoption of similar stances by those courts, and if these stances present enough similarity to qualify a European approach. In any case, if it comes out that, indeed, on the substance a similar substance is to be found, it will be necessary to keep in mind that this substance, depending on the legal order providing it, will find the enforcement method previously presented.

[62] Srl CILFIT and Lanificio di Gavardo SpA v Ministry of Health, No. Case 283/81 (ECJ 6 octobre 1982).

2. THE LIMITATION OF PERSONAL DATA PROTECTION AGAINST MEASURES FOR PURPOSE OF NATIONAL SECURITY UNDER A TWO HEADED CONTROL

This part aims to present how European states' acts that protect national security, and at the same time limit the protection of data subjects' rights are controlled by European Courts to ensure the enforcement of the right to personal data protection. Indeed, no textual sources provide a sufficient "toolbox" to determine the arbitration that must be made between those two notions depending on the circumstances. In the space of indefinite regulation, a range of possibilities lies that the European judges must clear. In that space, they fully embody their role of arbitrator between opposed imperatives. There, they are back to the roots of their function: to proceed to the fair share of the responsibilities. Because of their role of interpreter of legislation unipotent to frame at a European level the arbitration to make, in legal order where legislators aren't empowered to address the problem directly, they are the ones called to place the limit between the states willing to interfere into human rights to protect national security. In this mission, their main tool is the control of proportionality. Indeed, as Weiss states: "the principle of proportionality serves as the overarching analytical tool, [it] determine the effective level of human rights protection"[63]. Hence, it's precisely the case law of the two supranational courts, in the absence of common political will to lay down common rules to arbitrate between the interests of data protection and national security, that is to forge the European approach through the control of proportionality.

Classically, in human rights protection, the proportionality test is an overarching tool. Used by both courts as they protect human rights, they have, however, their interpretation of that test. It leads in the end to the demonstration of a plurality of proportionality test. Consequently, each subpart will analyse separately the case-law of the ECtHR and the ECJ, to study how they develop their proportionality test, and the substance of their control. In other words, this part seeks, for each case law to reveal how limitations brought to the right of personal data protection for purposes are reviewed.What is common thought is that due to the high sensitivity of such subjects, courts were influenced to adapt. The question then is, to what extent did the national security imperatives influence the argumentation of the ECtHR, in its enforcement of its convention? The second question is: how can we qualify the stance adopted by the courts in such matters? Despite the

[63] Wolfang Weiss in "Fundamental Rights in the EU - A matter for two courts"; Sonia MORAN-FOADI & Lucy VICKERS; Bloomsbury; 2017; p71.

precisions brought by extensive secondary legislations, which could have led one to think of a limited role of the CJEU in interpreting that law, CJEU is still in a proportionality intellectual set-up. To finish, this part, a third subpart will be dedicated to the study of the main discrepancy and common grounds of both case law.

2.1. Analysis of ECHR's case-law

ECtHR case law interprets a less substantial regime of personal data protection than the CJEU. In this regime, and contrary to the CJEU, no provision supports the possibility of the exclusion of ECHR's rights application. Hence, national security concerns can only limitation the application of Article 8, under the proportionality principle. This leads to the second point of our focus on ECtHR's case law analysis. Due to the immense power of processing new tools and AI that can be put into action by domestic legislation, the possibility of abuses of these legislations is also immense. The Court highlights this by describing mass surveillance as a field: "where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole"[64], where therefore greater guarantees against abuse are required. However, despite the massive threat caused by mass surveillance over human rights, the ECtHR still recognises to the States parties to the Convention a broad margin of appreciation when it comes to national security. Indeed, as the threats of a present context are highly present and resourceful, the Court states: "Given the present-day threats of global terrorism and serious cross-border crime, as well as the increased sophistication of communications technology, the Court held that Sweden had considerable power of discretion ("a wide margin of appreciation") to decide on setting up such a system of bulk interception"[65]. In that matter, the recurse to secrecy is considered legitim.[66]

[64] Roman Zakharov v. Russia, No. 47143/06 (ECtHR [GC] 4 décembre 2015), par. 233.
[65] Centrum För Rättvisa v. Sweden, No. 35252/08 (ECtHR [GC] 25 mai 2021), par. 178, to see also par. 237.
[66] Centrum För Rättvisa v. Sweden, No. 35252/08 (ECtHR [GC] 25 mai 2021),par. 236

2.1.1. Requirements set up by the ECtHR, a framework to enable control by independent national authorities.

Under article 8§2 ECHR: "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security […]". Therefore, the ECtHR, when assessing the proportionality of a legislation infringing personal data protection for the purpose of national security, analyses three criteria: the *source* of the limitation, the *necessity* of such limitation, and the *adequation of such limitation with a legitim objective*: here, national security.

Very early in its case-law the Court recognised that national security allows for a broad margin of appreciation to the States parties to the Convention. Indeed, in *Klass and others v. Germany* the Court pointed out that: "the domestic legislature enjoys a certain discretion"[67]. In *Big Brothers and others v. UK,* the Court precised: "The Chamber expressly recognised that States enjoyed a wide margin of appreciation in deciding what type of interception regime was necessary to protect national security but considered that the discretion afforded to States in operating an interception regime would necessarily be narrower"[68].Here lay an important point: the ECtHR seems to distinguish two different regimes of control, first one related to the conception of the interception legislation, and the second related to the application of its legislation by State's competent authority: for example the intelligence service.

Indeed, as shown in the precedent part, the secrecy of national security measures challenges the common conception of judicial review. Indeed, as the individuals can't demonstrate a direct affection, the ECHR had to soften its admissibility criteria. However, this answer only partly the problem of lack of judicial review because, even though the ECtHR lays down a regime for the States parties to the convention to respect when designing their legislations, the possibilities for a control *in concreto*, on the factual measures of surveillance, remain restricted. Indeed, since those measures are being led in secrecy, it is logically difficult for an individual to be aware of it, and to contest them. This was a concern that led the ECtHR to develop throughout its case law exigence

[67] Klass and Others v. Germany, No. 38581/16, 41914/16, 57510/16, 62644/16, 7190/17, 10973/17, 12530/17, 19411/17, 22087/17, 28475/17, 78165/17 (ECtHR 6 septembre 1978) p49
[68] Big Brother Watch and Others v. the United Kingdom, No. 58170/13, 62322/14, 24960/15 (ECtHR [GC] 25 mai 2021), par. 274

related to the control of the application of the legislation, completing the *a priori* control of the legislation.

This *a priori* control, made by the ECtHR is in no way comparable to what the Strasbourg's judges are used to do in deciding other cases. The peculiar sensitivity of the interests at stake, led the ECtHR to recognise a wide margin of appreciation to the Contracting Parties. Even more, it led the Court to firmly bend the framework of its method, almost to the denaturation of the classic proportionality test, keystone of the human rights judges. Indeed, the ECtHR's judges are "required to examine the proportionality of the [relevant] legislation itself and the safeguards built into the system allowing for secret surveillance, rather than the proportionality of any specific measures taken in respect of the applicant."[69]As mentioned before, the Court adapts its control to the peculiar situation of surveillance legislation: performed in secret, it's hard to contest the measures taken in application of a national security legislation, only stand that law to confront the applicant's claim. For example, as bulk interception measure will be led in secret, an individual can't contest this particular measure, he can only contest the legislation allowing for such interception to be undertook. This control is very different from the proportionality control the Court is used to do in its case-law, as provided notably by Article 8-2 ECHR, and ends up looking more like an adequacy test, or maybe even a rule of reason.

However, what's common is that "the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference"[70]. Indeed, margin of appreciation must not lead to arbitrary. That's why, even when the domestic legislation grant discretion to national authorities, these ones must have a definite scope of action to avoid arbitrary. Hence, to frame the Contracting Parties in the definition of their legislation on bulk interception, a list of 8 criteria has been provided by the ECtHR in *Centrum for Rattvisa*[71]*:*

"*The Court will examine whether the domestic legal framework clearly defined:*

[69] Kennedy v. the United Kingdom, No. 26839/05 (ECtHR 18 mai 2010), par.155.
[70] Guide to the Case-Law of the of the European Court of Human Rights Data protection Updated on 28 February 2023, §93, https://ks.echr.coe.int/documents/d/echr-ks/guide_data_protection_fre
[71] Centrum För Rättvisa v. Sweden, No. 35252/08 (ECtHR [GC] 25 mai 2021). par.275

- *The grounds on which bulk interception may be authorized;*
- *The circumstances in which an individual's communications may be intercepted;*
- *The procedure to be followed for granting authorization;*
- *The procedures to be followed for selecting, examining, and using intercept material;*
- *The precautions to be taken when communicating the material to other parties;*
- *The limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;*
- *The procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;*
- *The procedures for independent ex post facto review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.* »

It is possible to notice here that the first six criteria are dedicated to precising the reasons, the grounds, and the conditions under which interception can be undertaken, and that the last two provide for supervision of the processing and its review. The supervision must be made by an authority that reassemble two qualities: being independent, and powerful enough to address "the instances of non-compliance". No more precision is brought so it's possible to affirm that a non-jurisdictional entity can be called to carry such mission, as long as it is an independent authority invested from the power to put a term to an infringement. Overall, the first six criteria have for aim to enable for independent control of these latter.

Thus, these six criteria allow not only the ECtHR to conduct a test that takes more from the compliance test rather than a proportionality test, as the Strasbourg's judges are used to perform, this latter being "delegated" to the independent authorities in charge of the supervision et "ex post facto" review at the national level. Indeed, related to the first criteria of the aforementioned list, the Court states: "In sum, the grounds upon which bulk interception can be authorised in Sweden are clearly circumscribed so as to permit the necessary control at the authorisation and operation stage and ex post facto supervision"[72]. Hence, the criteria that the ECtHR lays down aren't so much for the proportion but it's really to ensure the national authorities are able to control.

[72] Centrum För Rättvisa v. Sweden, No. 35252/08 (ECtHR [GC] 25 mai 2021), par.288

The principle of subsidiarity is the main reason behind this list of criteria. This control is respectful of the subsidiarity principle and of the sovereignty of the states. In fact, the Court only controls the adequacy of the legislation to create a framework for the national security to be protected, which, in the same time, must guarantee that no disproportionate limitation to personal data protection would occur. By accepting that, the Court, in the end, tolerates that article 8 will be limited for national security. The ECtHR only seeks to ensure that the limitation is really undertook for national security motives, and that the parties to the convention won't use the secrecy of the system to broaden surveillance, or to launch an excessive surveillance.

This method is similar, to some extent, to what the EU would do with a directive laying a minimal harmonisation. Indeed, the case law of the ECtHR lays down necessary criteria for the national legislator to design its law with one principal aim to ensure a review, at least by an independent authority, for the better by a judicial authority. Indeed, as judicial review is a key component of the rule of law, it must be ensured even in the context of national security. The obligation laid down by the two last criteria represents the ECtHR's will to institute an "end-to-end" control of the interception measures, "meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken"[73]. It's an idea of a continuous control over the interception, made even more necessary as the gravity of interferences are increasing at each step of the surveillance. Indeed, "The Court views bulk interception as a gradual process in which the degree of interference with individuals' Article 8 rights increases as the process progresses"[74]. Such renewed control is even more justified by the fact that, due to national security concern, it's unlikely that the individual subject to surveillance will be ever notified of such surveillance, whether it's to protect the surveillance purpose, or because the authorities don't know his exact location — it would be the case for example of an individual located abroad. It is these reasons that led the ECtHR to affirm: "The Court considers that a remedy which does not depend on notification to the interception subject could also be an

[73] Centrum För Rättvisa v. Sweden, No. 35252/08 (ECtHR [GC] 25 mai 2021), par. 264
[74] Big Brother Watch and Others v. the United Kingdom, No. 58170/13, 62322/14, 24960/15 (ECtHR [GC] 25 mai 2021), par. 325

effective remedy in the context of bulk interception; in fact, depending on the circumstances it may even offer better guarantees of a proper procedure than a system based on notification"[75].

This framework instituted on bulk interception is an enhanced version of what was to be applied in matter of criminal investigation[76]. It is possible to affirm that this framework should be applied to every situation where the measure involved is led in secrecy, to protect national security. Indeed, it is because the lack of concrete elements, due to the secrecy of the missions, that hinder the ECtHR to perform a regular control of proportionality and force the Court to delegate to national authorities the task to perform the review. Indeed, the Court stated "*Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights*"[77]. In a matter where the secrecy is no more, where the Court is given sufficient amount of concrete information, it is legitimate to think that the Court will perform an *in concreto* analysis.

2.2. Analysis of the CJEU case-law

Within EU legal order, primary law provides for a method to review the legality of the limitations to the rights protected by the Charter. Indeed, Article 52§3 affirms that limitation will be tolerated to the conditions that they have a legislative basis, if they respect the essential substance of Charter's rights, and if they are proportionate. If Article 8 CFREU is subject to such a regime, the European legislator also precises the condition to limit the rights provided for by secondary law by restraining the number of motives for which a limitation could be implemented. Article 23 GDPR, 1., establishes a limited list of goals the following of which can justify limitation to the provisions this regulation carries. Among them are: national security (a), national defence (b), public security (c), prevention and repression of criminal acts (d). It's already possible to notice the degree of precision adopted by the EU legislator, which distinguished between notions that

[75] Centrum För Rättvisa v. Sweden, No. 35252/08 (ECtHR [GC] 25 mai 2021), par. 272.
[76] Centrum För Rättvisa v. Sweden, No. 35252/08 (ECtHR [GC] 25 mai 2021), par. 249
[77] Centrum För Rättvisa v. Sweden, No. 35252/08 (ECtHR [GC] 25 mai 2021), par. 250

could be, at first sight, understood as covering the same facts. Later on, it will be shown that the CJEU hierarchised theses grounds, to the contrary of the ECtHR (see supra 2.3).

The CJEU, to frame MSs' limitation made to personal data protection for purposes of national security, starts by clarifying a consistent contradiction within EU secondary legislation. Indeed, the Court solves the question of whether national security concern is a motive to the exclusion of EU law's application, or only a motive to limit the intensity of its application. Not without difficulty, the CJEU built a distinction between activities that fall under EU law, and, consequently, where a MSs' legislations can be reviewed, and those that, by nature, excludes EU law's application. The first section seeks to demonstrate that, even if such interpretation of the exclusion clauses allows for EU law to be applied broadly, the reasonings behind it isn't free of any means of criticism. The second has for purpose to demonstrate the regime the MSs have to respect when limiting the protection of personal data for national security purposes.

2.2.1. The restrictive interpretation of EU law exclusion provisions

A contradiction raises from recitals and articles providing the non-application of the EU law to situations belonging to national security concerns, and articles that provide only for the possibility offered to the MS to limit the protection on concern of national security. The exclusion is based on Recitals 16, Article 2(2)a for the GDPR, on recital 11 and Article 1(3) for the E-privacy directive, on recital 14 and Article 2(3)a for the LED. On another hand, limitations are provided by Article 23(1)a. for the GDPR, on article 15(1) for the E-privacy directive, and are spread out throughout different articles in the LED.

If national security exceptions are always provided by the legislations, their contents however, differ both from the wordings and from their interpretation. In interpretating GDPR's exclusion provision, and to protect the *effet utile* of the GDPR, the CJEU interprets strictly the notion of national security: "That exception to the applicability of the GDPR must, like the other exceptions laid down in Article 2(2), be interpreted strictly"[78]. Hence, the Court states: "must be regarded as

[78] Proceedings brought by B, No. Case C-439/19 (ECJ 22 juin 2021), par.61

being designed solely to exclude from the scope of that regulation the processing of personal data carried out by State authorities in the course of an activity which is intended to safeguard national security or of an activity which can be classified in the same category", to the exclusion of the activity that are characteristic to the States but not corresponding "to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities"[79].In matter of GDPR, MS must prove that the data processing is used in matter of national security, without any use in criminal proceeding to benefit from the exclusion of article 2(2)a.

In *Ligue des droits humains*[80], the CJEU precised the coordination of the exception provided by the *GDPR* and *Criminal proceedings* directive. In that Case, the Luxembourg Court adopts a restrictive interpretation of the exception provision laid down by Article 2(2)d GDPR. Based on recital 16, the judge states that, as the exception is mainly for processing undertaken in the context of criminal proceedings, including those for national security, their nature: criminal law measures, makes them within the *ratione materiae* directive's scope of application. This interpretation is logical because, article 2(2)a already provide for the logical exception of the field not covered by EU law. Hence, this Article2(2)d, is not so much an exclusion the Eu law protecting personal data, simply a provision design to ensure the application of a *lex specialis*: the *criminal proceedings* directive. This last also have provisions leading to the exclusion of its applications, in two situations. The first is that the directive won't be applied to the data processing undertaken in fields outside EU law isn't applicable. The second is that the directive doesn't apply to the processing undertook by EU's institutions.

The recognition of an overlapping between the exclusion and limitation provision within the E-privacy directive led to a series a case-law in which, unsurprisingly, the Court limits the possibility for the MS to use the exception. Recognised in *Telia2sverige* case and emphasized in *Quadrature du net*, the CJEU addressed the difficulty flowing from the contradiction between provision of

[79] La Quadrature du Net ea contre Premier ministre ea, No. Affaires jointes C-511/18, C-512/18, C-520/18 (Cour de justice 6 octobre 2020). par. 135
[80] Ligue des droits humains ASBL v Conseil des ministres, No. Case C-817/19 (ECJ 21 juin 2022).

exclusion and provision of limitation in the e-privacy directive. The CJEU stated': "an interpretation of that directive under which the legislative measures referred to in Article 15(1) thereof were excluded from the scope of that directive because the objectives which such measures must pursue *overlap substantially* with the objectives pursued by the activities referred to in Article 1(3) of that same directive would deprive Article 15(1) thereof of any practical effect"[81]. Hence come the question: how can we distinguish the first from the second? Formulated in other words: How do we qualify a situation as belonging exclusively to the national security matter, a situation that won't see the application of EU law. When interpretating principle and exception, it is broadly admitted that a principle's exception should be interpretated strictly to protect the effectivity of the said principle[82].

The ECJ built, not without difficulty, a distinction within this overlapping. The difficulty here comes from the fact that the activities referred to in the provisions "*overlap substantially*"[83], a being recognised by the CJEU very early in its case-law. This overlapping brings confusion between multiple potential solutions for the same case. Indeed, opposed parties to a case can both used this different provision to different purposes, a Member States to not have the EU law applicable to its case, plaintiff to see the national legislations controlled under a proportionality test. Thus, the CJEU had to resorb this overlapping. Today's regime comes from the *Quadrature du Net* case law[84] In that case, the Court, inspired by its own case law[85], presented again a reasoning around the notion of the *effet utile* of EU law. It affirmed that, recognising the application of the exclusion provision of the case would deprive Article 15(1) from all *effet utile*. However, it is also possible to affirm that, in refusing the application of the exclusion provision, the Court necessarily deprives Article 1(3) of all *effet utile*. It must be recognised that this interpretation is consistent with CJEU's ancestral method of interpretation, that leans to ensure the

[81] La Quadrature du Net and Others v Premier ministre and Others, No. Joined Cases C-511/18, C-512/18, C-520/18 (ECJ 6 octobre 2020), par.97
[82] Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, No. Joined Cases C-293/12 and C-594/12 (ECJ 8 avril 2014). §52 ; GD contre Commissioner of the Garda Síochána ea, No. Affaire C-140/20 (Cour de justice 5 avril 2022 §40
[83] La Quadrature du Net and Others v Premier ministre and Others, No. Joined Cases C-511/18, C-512/18, C-520/18 (ECJ 6 octobre 2020), par.97
[84] La Quadrature du Net and Others v Premier ministre and Others, No. Joined Cases C-511/18, C-512/18, C-520/18 (ECJ 6 octobre 2020).
[85] Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, No. Joined Cases C-203/15 and C-698/15 (ECJ 21 décembre 2016).

effectiveness and primacy of EU law. To assess whether this restricted interpretation of the exclusion provision effectively deprives this last from all *effet utile*. To do so, attention must be brought on the second argument of CJEU in that case.

The CJEU, due to the lack of persuasive strength of this argument, as well as the efficiency of the MS' counsels who made a reference to a 2006 case law[86] involving the EP against the Council and the EC, obliged the ECJ to develop a better motivation. Indeed, in the interest to obtain the exclusion of the e-privacy directive to their situations, the Member states invoked the said case law because of its solution, which concluded to the exclusion of EU law's application. About that 2006's case, the Court stated[87] that, if it excluded directive 95/46 from being applied to the case, it was because the transfer in question "fell within a framework established by the public authorities relating to public security ». However, this argument, once again, presents flaws. Indeed, how not to see in the fact of *Quadrature du Net* a "framework established by the public authorities relating to public security" since the contested legislation "require electronic communications operators and technical service providers to 'implement on their networks automated data processing practices designed, within the parameters laid down in the authorisation, to detect links that might constitute a terrorist threat'"[88]. Hence, the CJEU went further with its argumentation. The reasoning of the CJEU was the following: as the Article 1(3) applies to the activities of the telecom companies, and as the regulations of the said telecom companies fall can be addressed as limitation provided by Article 15, those companies, when transferring data to the MS's authorities, are processing data in the field of application of the e-privacy directive. Secondly, the Court states on whether the exclusion provision is applicable to the case. The CJUE states that, this processing, as it flows from a regulation addressing private sector, can't be seen as characteristic of states. Here the Court, use a subjective criterion, unfound in the directive, instead of the material criterion provided for by the EU legislator.

[86] [European Parliament v Council of the European Union (C-317/04) and Commission of the European Communities (C-318/04), No. Joined cases C-317/04 and C-318/04 (ECJ 30 mai 2006).]
[87] La Quadrature du Net and Others v Premier ministre and Others, No. Joined Cases C-511/18, C-512/18, C-520/18 (ECJ 6 octobre 2020), par 100.
[88] La Quadrature du Net and Others v Premier ministre and Others, No. Joined Cases C-511/18, C-512/18, C-520/18 (ECJ 6 octobre 2020), par 57.

This change can be justified by the imprecision of the directive that make the material criterion ineffective. However, the subjective criterion wasn't use in EP v. Council 2006 where the situation was quite similar: aerial compagnies were transferring data to the MS, for purpose of public security — which is, by the way, a less important motives compared to national security, according to the Court in the same case. This creation strongly changes the stance of the CJEU on the matter, to the extent where it can be seen as a revision of jurisprudence[89]. Instead of recognising a revision of its case law, the CJEU justify by claiming that the two legislations, directive 95/46 in one hand, and E-privacy directive another hand are different. In paragraph 101, the Court provides the following argumentations: the interpretation of 95/46 directive's exception didn't call for a distinction based on the implication of private sector[90]. On the other hand, and in the same paragraph, the Court states: "by contrast, in the context of interpreting Article 1(3) of Directive 2002/58, it is necessary to draw such a distinction". To the demonstration of that *necessity,* the CJEU affirms: "all operations processing personal data carried out by providers of electronic communications services fall within the scope of that directive, including processing operations resulting from obligations imposed on those providers by the public authorities". However, this is simply logical as the exception provided by article 1(3) only excludes from the application of the directive, the activities based on national security and does no distinction on what kind of processing is used. In other words, the criteria of the directive is finalist while the ECJ keeps using the subjective criteria. Overall, in stating as such, the ECJ disqualifies all activities involving private sector from claiming the national security exception.

In the same paragraph (par.101), the Court finishes to justify it by describing the exception of 95/46's exception as having a broader wording in comparison to 2002/58's exception. However, a quick look to those wording contradict this; while the 95/46's article 3(2) first indent states:

> "*2. This Directive shall not apply to the processing of personal data:*
>
> *- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to*

[89] Tzanou, Maria, et Spyridoula Karyda. « Privacy International and Quadrature Du Net: One Step Forward Two Steps Back in the Data Retention Saga? » EUROPEAN PUBLIC LAW, s. d.)
[90] La Quadrature du Net and Others v Premier ministre and Others, No. Joined Cases C-511/18, C-512/18, C-520/18 (ECJ 6 octobre 2020), par.101

processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law";

Article 1(3) of 2002/58 directives states:

"*This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law*".

2.2.2. Analysis of the limitation regime

In the interpretation of the Charter, the CJEU finds the regime applicable to charter's rights limitation. It is provided by article 52(1) CFREU, which is worded as following: "*Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.*" From this wording, it's possible to understand that, the CJEU, when assessing the conformity of a limitation to a right protected by the Charter, takes into account the following criteria: the legal origin of the limitation, the respect of the Charter's rights essences, and, in the context of "the principle of proportionality", the adequacy of the limitation to protect, either a general interest of the EU or the rights and freedom of others, and, whether the limitation is necessary to complete objective.

The CJEU, in interpretating Article 8 CFREU, never gives a positive definition of the essence of the right protected by this article. Instead, the Court analyses, each time, if this criterion is respected by the legislation reviewed, and, in doing so, gives a negative definition of what would reach the essence of personal data protection. Hence, the analysis of the case law gives the following information.

In *Digital rights Ireland,* after providing in par. 39 that the absence of access to the content of the communication precludes to recognise an infringement of Article 7's right essence, the Court states in par. 40: *"Nor is that retention of data such as to adversely affect the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter, because Article 7 of Directive 2006/24 provides, in relation to data protection and data security, that, without prejudice to the provisions adopted pursuant to Directives 95/46 and 2002/58, certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or of public communications networks. According to those principles, Member States are to ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data"*.

From this extract, it is possible to understand that, for the Court, the essence of article 8 relays on the respect of principles related to data protection and data security such as: the existence of "appropriate technical and organizational measures […] adopted against accidental or unlawful destruction, accidental loss or alteration of the data". From this wording, it's remarkable that only the protection of the data itself, its content, belong to the content of Article 8's essence. Hence, with this wording, it is arguably possible to affirm that any infringements to personal data protection will never be considered as infringing article 8's essence, as long as they don't cause any harm to the data's integrity.

In *Telia2Sverige,* the CJEU analyses only briefly the satisfaction of that criteria and identifies to both article 7 and 8 of the Charter the substance attributed only to Article 7 in *Digital Rights Ireland*: "*So far as concerns the essence of the fundamental right to privacy and the other rights laid down in Article 7 of the Charter, it must be held that, even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with those rights, it is not such as to adversely affect the essence of those rights given that, as follows from Article 1(2) of the directive, the directive does not permit the acquisition of knowledge of the content of the electronic communications as such*"[91].

[91] Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, No. Joined Cases C-293/12 and C-594/12 (ECJ 8 avril 2014), par. 39.

Hence, after recognising in par. 100 the "*very far reaching*" interference in the rights protected by Articles 7 and 8, the Court provides in par. 101 that this interference doesn't cause harm to the essence of those rights — hence both Articles 7 and 8 — to the extent that "*such legislation does not permit retention of the content of a communication*". It is a logic statement from the Court as one could already have been surprised to not see Article 8's right essence mentioned alongside Article 7 in *Digital Right Ireland.*

In *Ligue des droits humains* case law, the Court affirms that the PNR's interferences with Articles 7's and 8's rights don't infringe the essence of the rights protected by those articles. As justifications, the Court takes into account the facts that "*the data covered by that directive do not by themselves allow for a full overview of the private life of a person*", that PNR directive "*circumscribes the purposes for which those data are to be processed*", and "*lays down the rules governing the transfer, processing and retention of those data as well as the rules intended to ensure, inter alia, the security, confidentiality and integrity of those data, and to protect them against unlawful access and processing*"[92]. Here, the requirement of data's integrity protection calls into action the need for cybersecurity. Hence, it's for the MSs, to comply with the essence of Article 8's rights, to develop information system security. To do so, MSs don't have full margin of manoeuvre. Indeed, they are bind notably by the NIS 1 directive, which is the first instrument of hard law harmonizing the cybersecurity in EU[93].

In *Opinion 1/15*[94], the CJEU states : "*As for the essence of the right to the protection of personal data, enshrined in Article 8 of the Charter, the envisaged agreement limits, in Article 3, the purposes for which PNR data may be processed and lays down, in Article 9, rules intended to ensure, inter alia, the security, confidentiality and integrity of that data, and to protect it against unlawful access and processing*"[95]. In that opinion, the Court reaffirms already known criteria: the existence of limits to the purposes for which PNR data can be processed, criteria to be found in *Ligue des droits humains case*, and the requirement of data security, in the continuity of *Digital*

[92] Ligue des droits humains ASBL v Conseil des ministres, No. Case C-817/19 (ECJ 21 juin 2022). §120.
[93] Karathanasis, Theodoros. « Member States Confronted with EU-Based Rules in the Field of Cybersecurity, The Effectiveness of Directive (EU) 2016/1148 ». Phdthesis, Université Grenoble Alpes [2020-....], 2022. https://theses.hal.science/tel-04077226. P.45
[94] Opinion of the Court (Grand Chamber) of 26 July 2017. Case Opinion 1/15. (ECJ 2015).
[95] Opinion of the Court (Grand Chamber) of 26 July 2017, par. 150.

Right Ireland. However, the CJEU's case also changed in time. Indeed, since *Digital Right Ireland*, the requirement of the protection against accidental loss became protection of the confidentiality, including the necessity to protect from external intrusion. Moreover, and more notably, the Court considered the provisions of rules indented to ensure, beyond the security of the data, the lawfulness of the processing.

Considering this case law in four stories, it's nowadays still quite difficult to define in a comprehensive manner the essence of Article 8's rights. In *Digital Rights Ireland* and *Opinion 1/15*, Articles 7 and 8 were addressed separately, in *Telia2Sverige* and *Ligue des droits humains* instead, they were addressed together. The fact that the CJEU address simultaneously these two notions is notable as long literacy has been dedicated to the mission of identifying the distinction between these two rights[96]. Anyhow, due to the casuistic method employed by the Court, it's only possible to affirms that the essence of Article 8's rights would be adversely affected by a legislation that doesn't provide limits to data processing, or guaranties of data's integrity protection. In the end, this finding is to be put in perspective with the fact, that, sometimes, the Court simply doesn't check whether the essence of Article 8's right is infringed.

Indeed, in *Ministerio fiscal*, *La Quadrature du Net*, *Privacy international*, *Proceedings brought by B., G.D v. the commissioner*, the CJEU doesn't address the question of whether the essence of this Charter's right has been infringed. The motive for such abstention is questionable. One could support the idea that, considering the previously presented finding on the Article 8 essence, this step is not so useful to the protection of this Article's right. The author tends to disagree with that idea to the extent that, the rights's essence protection has a different finality compared to the necessity criteria. Indeed, the essence of a right is an essential, a sacred aspect of that right that the CJEU must protect. For that purpose, the protection of an *essential* aspect of a right, the control of proportionality is irrelevant. Indeed, the control of proportionality only seek to answer whether an interference is necessary or proportionate. On the other, hand the protection of the essential aspect of the right is that, *per se*, this essential aspect cannot suffer from any kind of limitation, even the softest one. Hence, the aspects of Article 8's essence, as presented by the Court before, seem irrelevant to the extent that they introduce limitations to the interferences that can be made, but is

[96] Brkan, Maja. « The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors ». Maastricht Journal of European and Comparative Law 23, nº 5 (2016): 812-41.

unipotent to identify an aspect of Article 8 to sacralise. In any case, in these situations, it participates for a greater possibility offered to MS to limit personal data protection. Indeed, it's a criterion in less to assess the legality of the national measure.

However, *Data protection commission v Facebook Ireland and Schrems* presents a peculiarity. Indeed, in this case, which review USA's adequacy decision, the CJUE doesn't use use strictly the criteria from Charter's Article 52§1. Indeed, the GDPR only requires an adequacy, and equivalence, and not the same level of protection. Hence, the question is not strictly if the thirds state legislation complies with our criteria but if the criteria used by other countries offers similar protection than our: "that article [Section 702 of FISA, which provides for an annual certification given to specific authorities to conduct surveillance programs,] cannot ensure a level of protection essentially equivalent to that guaranteed by the Charter"[97]. Here, the CJEU does not assess the conformity of the US legislation with article 52§1 tools, instead the Court search if USA's legislation delivers an equivalent protection that what Article 8's interpretation provides.

The principle of proportionality, in EU legal order, "requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives"[98]. Furthermore, in that specific matter of personal data protection, the CJEU affirms, to the contrary of the ECtHR, that the legislator's discretion is limited, justifying a stricter control from the CJEU. Indeed, the Court states in *Digital rights Ireland* (§47-48) : "*With regard to judicial review of compliance with those conditions, where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference*". This finding resonate peculiarly as the ECtHR is sometimes depicted as the more human rights protecting of the two. For example, "Weiss argues that whilst the ECtHR was already a human right court by virtue of its intensified proportionality control, the CJEU has tentatively taken first

[97] Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, No. Case C-311/18 (ECJ 16 juillet 2020), par 180

[98] Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, No. Joined Cases C-293/12 and C-594/12 (ECJ 8 avril 2014), par. 64 and case law cited.

steps on this path, but it is still tempted to continue traditional interpretative approaches due to its structural characteristics"[99].

As preliminary development to the presentation of the limitation regime drawn by the CJEU, it must be mentioned that Luxembourg judges stated that, national security concerns is the highest exception, the one that allows the wider limitations to the rights protected by article 7, 8 CFREU. As it is a very sensitive exception, the CJEU distinguishes national security from similar but divergent notions. Therefore, are seen as different and having less "justifying power" public security concerns and imperatives flowing from the fight of organised criminal activities : "the importance of the objective of safeguarding national security, read in the light of Article 4(2) TEU according to which national security remains the sole responsibility of each Member State, exceeds that of the other objectives referred to in Article 15(1) of Directive 2002/58, inter alia the objectives of combating crime in general, even serious crime, and of safeguarding public security"[100]. Those are the only concerns, beside national security, justifying acute limitations: "only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter"[101].

Hence, as it is an exceptional motive, it's under the objective of safeguarding national security that the CJEU tolerates the most acute interferences with article 7 and 8 CFREU. Its case-law is synthetized within a series of case law consecrated by *Quadrature du Net*.

The repercussions of the *Digital Rights Ireland* ruling are noteworthy, given the Court's firm censure of the "vast and particularly serious" intrusion perpetrated by the Directive. This ruling is even more important today as MSs tends to rely more on big data analysis than human intelligence to protect their national security[102].

[99] Fundamental Rights in the EU - A matter for two courts ; Sonia MORAN-FOADI & Lucy VICKERS ; Bloomsbury ; 2017 ; p.4
[100] GD v The Commissioner of the Garda Síochána and Others, No. Case C-140/20 (ECJ 5 avril 2022), par.57
[101] GD v The Commissioner of the Garda Síochána and Others, No. Case C-140/20 (ECJ 5 avril 2022), par.59
[102] Tinière, Romain, Claire Vial, et Frédéric Sudre. Droit de l'Union européenne des droits fondamentaux. Collection Droit de l'Union européenne 16. Bruxelles: Bruylant, 2023. p431

In the aftermath of *Tele2sverige*, MSs are compelled to precisely target data for processing, restricting themselves to information that pertains to individuals likely to be linked, directly or indirectly, with acts of serious crime or terrorist enterprises. This targeting imperative extends to both the identification of metadata for storage and the terms of access. Crucially, this obligation demands prior scrutiny by a judicial body or an independent administrative authority, eliminating the possibility of broad, indiscriminate retention with unrestricted access for governmental entities.

In *La Quadrature du Net* case[103], the Court states again its stance and introduces a notable exception: the objective of safeguarding national security may justify more profound interference than what is tolerates to safeguard public security, the CJUE lays down the following criteria:

- limited period: the interference must be constrained within a specific timeframe.
- concrete circumstances: a MS must face sufficiently tangible circumstances indicating a real and present or foreseeable threat to national security. Importantly, the retention under such circumstances cannot be a systematic practice, as emphasized by the CJEU.
- procedural guarantees, there must be established procedural guarantees to protect individuals affected by the interference.
- Independent review: injunctions issued to service providers, in the context of safeguarding national security, must be subject to judicial review.

This nuanced approach by the Court recognizes the heightened sensitivity and importance of national security concerns, while concurrently emphasizing the necessity for clear safeguards and oversight mechanisms to prevent abuse and protect fundamental rights.

This analysis illustrates that the CJEU adopts a very protective stance in matter of personal data protection, and reduces the power of action of, not only MS's legislator but also EU legislator, to the extent that it can be affirmed that the CJEU substitutes its margin of appreciation to the

[103] La Quadrature du Net and Others v Premier ministre and Others, No. Joined Cases C-511/18, C-512/18, C-520/18 (ECJ 6 octobre 2020), from par. 137 to 139.

legislators'. This arbitration between the right to personal data protection and the imperative of national security isn't made by primary law. Hence, what is the legitimacy of the CJEU to state that personal data protection is more important than national security? Fundamentally, judges' task is to interpret the law and to be creative only when this last is silent. Here, there was no silence, and nonetheless, the CJEU chose to arbitrate, in a way that doesn't seem necessary to fulfil its mission. Moreover, in doing so, the CJEU overstep on political instances' function. Indeed, it is up to these last, and only them, to arbitrate between value, because they have, or are supposed to have, democratic legitimacy. Especially, the EP which is elected by the EU citizens. By doing so, we can affirm that, to some extent, the CJEU is the motor of the EU approach, as it is neglecting in matters of personal data, the natural restraint it should have in interpreting political choice. Prof. Bouveresse on that subject affirms that: "by choosing a full control on an appreciation it used to interpret with restraint, the judge substitutes its own appreciation to the one of the normative authorities, and, in doing so, annihilate the appreciation power of the competent authority"[104]. In doing so, the Court steps on the horizontal sharing of function within the EU, overstepping its judicial function to involve itself within the legislative function. Traditionally, as an inheritance of CECA's treaty, the CJEU limits its control on matters requiring a high level of expertise. For example, in a 1996 case Commission v. Council[105], the Court choose to restrict the intensity of its review because it recognised that the legislator had to evaluate, in the implementation of the agricultural policy, a "complex economic situation": "in reviewing the exercise of such a power the Court must confine itself to examining whether it contains a manifest error or constitutes a misuse of power or whether the authority in question did not clearly exceed the bounds of its discretion". Similarly, in another 1996's case, UK v Council[106], the Court stated: "As to judicial review of those conditions, however, the Council must be allowed a wide discretion in an area which, as here, involves the legislature in making social policy choices and requires it to carry out complex assessments", with the same consequences on the content of its control: absence of power's misuse, and no exceeding of legislator's discretion.

---

[104] Bouveresse, Aude. « Le pouvoir discrétionnaire dans l'ordre juridique communautaire ». Strasbourg 3, 2007, p.209. traduction on my own.

[105] Commission of the European Communities v Council of the European Union, No. Case C-122/94 (ECJ 29 février 1996), par.18.

[106] United Kingdom of Great Britain and Northern Ireland v Council of the European Union, No. Case C-84/94 (ECJ 12 novembre 1996), par. 58

Hence, it's possible to see here, once again, that the Court is adopting a very strict human rights protective stance. Indeed, it's possible to affirm that the limitation of personal data protection by the use of highly technical means to protect national security is a very complex matter where the legislator's discretion could be protected. However, despite this evident level of complexity the Court chose to restrict the margin of discretion of the EU legislator. Moreover, unlike the two cases previously presented, in which the Court acknowledged the need for restraint, the judges don't precise what precise extent it has on the content of the control.

Overall, the arguable illegitimacy of the Court to affirm the reduced margin of discretion of the EU legislator, in addition to the lack of transparency on the intensity of its control leads the author to qualify this situation as not satisfactory. Firstly, it is estimated that, while the correctness of Digital Rights Ireland's findings isn't to be questioned, the share of functions within the EU is damaged by such affirmation that the EU legislator is to find its margin of appreciation restricted; by doing so the Court extends its power further from what the EU primary law intended to confer. Furthermore, and more pragmatically, the absence of the Court's explanation on the effect of such a restricted margin of appreciation is not to help the EU legislator on the stance it should adopt. Doing so might discourage the EU legislator from making strong choice in complex matters, in other words: especially where the margin of appreciation is usually meant to be.

2.3. Complementarity and discrepancy between two different praetorian approach

On the grounds able to justify bulk interception, the ECtHR affirms: "*Article 8 of the Convention does not prohibit the use of bulk interception to protect national security and other essential national interests against serious external threats*". The ECtHR affirms in *Centrum for Rattvisa*[107]: "*the grounds upon which bulk interception can be authorised in Sweden are clearly circumscribed so as to permit the necessary control at the authorisation and operation stage and ex post facto supervision*". Here, the control performed by the ECtHR is limited to the analysis of the clarity of the law and doesn't carry a control on whether these grounds are justified.

[107] Centrum För Rättvisa v. Sweden, No. 35252/08 (ECtHR [GC] 25 mai 2021), par 288.

The ECtHR prohibits the use of the data gathered for national security purposes to the end of criminal proceedings, there must be compartmentalisation between the data collected for different end. This is justified because, even if data have been processed lawfully in the first place, to fights threats of terrorisms for example, the prolongation of the processing for other crime of less gravity purposes would be unjustified, according to the principle of proportionality of processing. Hence, the access from "traditional" police services to intelligence services database, if it's not *per se* forbidden, must be framed by sufficient guarantees. Indeed, in *Centrum for Rattvisa*[108], the CJEU stated that "The risk of signals intelligence being used outside the scope of foreign intelligence activities must be sufficiently contained by clear legal provisions and effective supervision."

However, it can be relativised to the extent that ECtHR welcomes the exclusion made by such legislation excludes the use of powers of surveillance in matter of criminal investigation: "*It is undisputed that information obtained through the impugned regime of signals intelligence cannot be used in criminal proceeding*"[109]. Hence, we can understand that, if the ECtHR recognized the possibility of bulk interception for motives other than national security, it, however, doesn't allow for *foreign intelligence services* to use the data collected in their area of competence for uses related to criminal proceedings. Indeed, the Court provides that the Swedish: "*section 4 of the Foreign Intelligence Act excludes the conduct of signals intelligence within foreign intelligence to solve tasks in the area of law enforcement or crime prevention*"[110]. However, it doesn't preclude national legislator to grant institutions in charge of fight against serious crime the right to recourse to bulk interception, in the context of their competences and with respect of ECtHR's criteria.

It is important to mention that the ECtHR doesn't provide a common definition of national security. Instead, the ECtHR requires that the grounds justifying bulk interception must be clear enough to preclude the discretionary power of the intelligence service to be used arbitrary.

On the grounds able to justify bulk interception**,** the CJEU developed a stricter control than the ECtHR on that question. Indeed, while the Strasbourg's judges entertain a formal control, the CJEU developed a distinction between serious crime, public security, and national security, each

[108] Centrum För Rättvisa v. Sweden, No. 35252/08 (ECtHR [GC] 25 mai 2021), par. 193
[109] Centrum För Rättvisa v. Sweden, No. 35252/08 (ECtHR [GC] 25 mai 2021), par.287
[110] Centrum För Rättvisa v. Sweden, No. 35252/08 (ECtHR [GC] 25 mai 2021), par.286

grounds having different "justifying power", and national security being the more important one, as mentioned before. The CJEU gave a description, if not a definition, of what national security implies, as a responsibility:

It "corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities"[111]. With such definition, national legislators find a restricted discretion in elaborating their bulk interception legislation.

Additionally, the question of initiative subsists. As the CJEU has shown itself very directive, and very liberal, we can truly question the margin of appreciation left to the EP in that matter, and the ability left to the Council to legislate in a way preserving MSs' interests to protect national security. In any case, these discrepancies simply illustrate that both courts don't beneficiate from the same directive powers to guide their members states to adopt a specific behaviour.

2.4. Summary

In analysing the ECtHR's case law, this thesis sought to illustrate how the peculiarity of national security imperatives caused the Court to adapt its control. Firstly, to avoid denying the access to its court, ECtHR's judges adopted a flexible interpretation of the personal affectation criteria. Indeed, as secrecy makes hard, if not impossible, for the individuals to contest measures directly affecting him, the ECtHR's analyse the general legislation providing for the limitation to the right to personal data protection. Such adaptation also affected the subject review which became, for once, the law itself of the States, requiring from it to ensure the control by national, accredited institutions, to assess the proportionality of this contested legislation application. However, if in

[111] La Quadrature du Net and Others v Premier ministre and Others, No. Joined Cases C-511/18, C-512/18, C-520/18 (ECJ 6 octobre 2020) par.135

the design of this legislation, Contracting Parties own a wide margin of appreciation, the control of the application of these laws, made by national authorities, must be strict.

Relatively to the CJEU, these developments sought to explain how the CJEU interpretates restrictively the exclusion provisions present in secondary law of the EU. It has been shown that the Court, by arguments unequally efficient, interpreted so strictly the exclusion provision that it can be very hard today for a MS's council to obtain from the Court the recognition that a given measure was taken solely for the purpose of national security. Such restrictive interpretation is coherent with the will of the Court to ensure EU law effectivity. However, it is possible to assess that, by extending so much the field of EU personal data protection law, the Court goes against the will of EU legislator. Moreover, such restrictive interpretation cannot be justified by the obligation for the CJEU to ensure the adequation between the protection offered by the ECtHR and its own, as the Strasbourg's judges themselves have a wide understanding of what is national security.

To conclude this part, it is possible to affirm that both the ECtHR and the CJEU provides to the States under their jurisdiction a framework to respect when designing their legislation. These regimes' aim is not to control in concreto what measures States are conducting to protect their national security. Instead, they have for purpose to make sure that national authorities will be able to control those measures. The goal is to ensure for a review at a national level, not necessarily judicial, but at least led by independent authorities. This control must be performed before and during the measures, in order to ensure for a "perpetual", or more rightly always renewed control of proportionality. When designing their frameworks, the CJEU is slightly more protective of personal data protection than the ECHR, by having a stricter definition of national security, and by reducing the margin of discretion of the legislators.

The first two part sought to demonstrate how the European Approach to the protection of personal data against measure seeking to protect national security is the conjunction of two supranational Courts' works: the CJEU and ECtHR. The following part will demonstrate the other side of the European approach, where, this time, personal data are protected for purpose of national security. Here, as national security is a regalian mission, one of the missions of the governing institutions, the judges don't have the first role. Here, it's the executive and legislative power that are to act, and, as this study looks for a European approach, the analysis is drawn to the EU. Indeed, the EU, because of to the competence it was granted with in matter of personal data, finds a privileged

place to initiate a European approach. Indeed, with the ordinary legislative procedure, the EU finds a way flexible tool to legislate for personal data protection and can legislate indirectly to protect personal data. One example is the recent directive[112] adopted to protect cybersecurity of essential infrastructure within MSs', another is the regulation of personal data processing on online services, to avoid disinformation and foreign influence in EU's democratic processes. The next part will be a case study of this last example.

[112] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), 333 OJ L § (2022). http://data.europa.eu/eli/dir/2022/2555/oj/eng.

3. THE DEFENCE OF PERSONAL DATA FOR PURPOSE OF NATIONAL SECURITY, CASE STUDY OF SYSTEMIC RISKS CAUSED BY ONLINE SERVICES

This part will be dedicated to the study of EU legislation to regulate online platforms and search engine, to prevent threat on national security. Here, and to the contrary of the previous development, national security isn't protected through the limitation of the protection of personal data but, to the contrary, by regulating their processing further. Brexit and Trump elections in 2016 have been under suspicion of mass manipulation of personal data. Companies such as *Cambridge Analytica* have been employed to process personal data to identify influenceable voters to target with personalised ads, with purpose to influence their vote for the benefit of a specific side. Apart from the ethical and obviously democratic problem that this method raises, it also has national security implications as foreign interests can be the backer of such campaigns. To the support of this idea, the EP called "the Member States to acknowledge the fact that foreign interference, including disinformation, is a national and cross-border security threat"[113].

Moreover, GDPR infringement can also lead to national security concerns when it flows from a foreign company has legal obligation to assist national intelligence effort. This is the case of Chines company *Bytedance*, owner of *Tiktok*. Indeed, under Article 7 of the Chinese 2017 Law on intelligence provide for citizens the obligations to "support, cooperate and collaborate in national intelligence work, and maintain the secrecy of national intelligence work of which they are aware"[114]. This risk led the EC and the Council to ban *TikTok* from the device of their employees. However, research within EU official documents database didn't allow to find official documents on these bans.

Hence, the following development will focus on the regulation by the EU of the activities of online providers to fight against foreign influence within the EU. A first section will be dedicated to the

[113] European Parliament resolution of 1 June 2023 on foreign interference in all democratic processes in the European Union, including disinformation (2022/2075(INI)) (2023). Par.11. http://data.europa.eu/eli/C/2023/1226/oj/eng.
[114] Institut Montaigne, « L'Europe et la 5G : le cas Huawei », Note, Mai 2019

study of the Digital Service Act[115] while a second while develop the proposal for a regulation of online political advertisement[116].

3.1. Systematic risks systematic of digital services, DSA's global framework

In the aftermath of the *Cambridge Analytica* business in Brexit referendum, and in Trump election in 2016, the EU legislators became aware of the need for a legal framework to the massive influence of internet actors. In simple terms, it's not possible to let personal data of Facebook users to be used to influence Europeans elections. Even more, those platforms: *X* (formerly Twitter), *Facebook*, *Instagram*, just to mention these, as they are housing growing contents with purpose of disinformation, or to stir hate, must have a control, a checking system on the content posted on their platform. These platforms have to raise their own "awareness" about their impacts on modern societies, and, as the DSA, provides must now act in consequences. Indeed, DSA requires from "very large online platform [VLOP] and very large online search engine [VLOSE]" to conduct systemic analysis of the impact of their services on the European society. To enforce, DSA's obligations toward those actors, the EC is empowered with surveillance and sanctions tools. Still in the legislative pipeline is the *Regulation on the transparency and targeting of political advertising*. This Regulation proposed by the EC on 11/25/2021 and modified in first reading on 02/02/2023, carries provisions related to an enhanced framework and set of obligations addressed to providers of online political advertising. In doing so, it addresses even more directly the issue of FIMI, its combination with the DSA carries interesting proposals. Far from pretending to exhaustivity, the incoming presentation will seek to present DSA's, and Regulation on political advertising's, main inputs in confronting the highlighted issue, namely: the need for increased protection of personal data against foreign influences in EU democratic processes.

---

[115] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance), 277 OJ L § (2022). http://data.europa.eu/eli/reg/2022/2065/oj/eng.

[116] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the transparency and targeting of political advertising (2021). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0731.

3.1.1. Analyse of DSA requirements and their addressees

The DSA lays down two main blocks of requirements in its Chapter III dedicated to "Due diligence obligations for transparent and safe online environment". The first one can be depicted as a common bloc of requirements. In this block, section I addresses globally all the intermediary services providers, and the following sections address more precisely different kind of providers distinguishing on the type of activity they are conducting. Section II provides obligations to "providers of hosting services, including online platforms", section III concerns exclusively the "providers of online platforms, while section 4 addresses "providers of online platforms allowing consumers to conclude distance contracts with traders". Some of the obligations laid down by the previous section see their application excluded to "micro and small enterprise". The second block of requirement, the relevant one to the problematic of our subject, can be qualified as an *enhanced block of requirements*. It tends to the anticipation and mitigation of systematic threats, some of them on national security of EU's MS; its provisions will be presented shortly. The common block of requirements lay down rules applicable both to "provider of intermediary services" and "providers of very large online platforms and of very large online search engines" while the enhanced block lay down obligation applicable only to those very large enterprises.

The distinction is made between intermediary service provider and very large provider. This distinction involves a material definition concerning intermediary service providers, and a quantitative criterion for the very large providers. Regulation Article 33(2) gives an objective criterion for the EC to define what a very large provider is: it is a provider that has a "number of average monthly active recipients of the service in the Union equal to or higher than"[117] 10% of EU's population. A provider matching this criterion will see itself address a decision from the EC under the provisions of article 33. This decision notifies the company that it is now subject to the application of the enhanced block of requirements, within a delay of 4 months.

[117]Article 33(2) DSA

3.1.2. Broad presentation of DSA's obligations.

The common block of obligations requires from all the service providers to show transparency in the conduct of their activities. For example, they must have clear and precise general conditions of utilisation that respect fundamental rights, such as freedom of expression (article 14). There is also the obligation of notification of any suspicion of criminal infractions, when those latter threaten people's life or security (Article 18), the obligation of transparency on the entity they are advertising for (Article 26), or the obligation to restrain from having recourse to the profiled advertisement when the providers have "reasonable certainty that the recipient of the service is a minor" (Article 28).

Section 4 of Chapter III, the enhanced block of obligation, provides to the very large service providers the obligation "to manage systemic risks". More precisely, they have to assess and mitigate, by themselves, systemic risks born from the use of their services (Articles 34 and 35). Moreover, they are under enhanced obligations regarding advertising (Article 39) and have a specific set of rules concerning the transparency report provided for by Article 15 (Article 42). To ensure the efficacity of this legislation, and in addition to the public and private enforcement system previously presented, very large service providers ought to conduct an annual audit under Article 37's conditions, and to constitute within their organisations a compliance function (Article 41).

The DSA provides two obligations that specially address the issue of personal data processing affecting the democratic process, which should be effective in to fight against FIMI. First, Article 26 lays down obligations to any "providers of hosting services, including online platforms", regarding the advertising services they are offering. These providers must allow service users to benefit from clear identification of what content is, in fact, an advertisement, and who is the sponsor of the said ad and/or the person beneficiating. Such information is important to allow these services' users to be aware of the content that is specifically targeted to them, and even more, to be aware of the content an entity wants them to see. In the context of our subject, they are especially useful are they would lower, in the author's opinion, the ability of FIMI to influence the ideas of EU citizens. Indeed, nowadays, disinformation is a very prominent problem, and this kind of regulation would limit the efficiency of disinformation campaigns.

Moreover, the providers must make accessible documentation allowing them to understand the mechanisms of individual targeting. Article 27 requires the providers to inform in their general

conditions on the techniques employed to recommend content to services' recipient, it'd be welcome for to legislator to go further than that. Indeed, it's possible to think that the lambda user won't be checking the functioning of the algorithms used by its social. However, for special, journalists, or whistle-blowers, this transparency would allow them to perform research and raises ethical questions that can be raised by the conception of algorithms, which are never neutral. For the same reasons presented before, such regulation would allow, in the end, user to be more aware of how their content is generated, and how they can be influenced, and confirmed in their idea. It would participate, here again, to reduce the effectiveness of disinformation when it is conducted by foreign entities.

The measures presented before are thought as capable of mitigating the risk of FIMI. Besides implementing those obligations, very large service providers are under obligation to, by themselves, identify and mitigate the risks their services can generate. VLOP are under obligation to fight against foreign influence as it is among the (non-exhaustive) list of risks provided by Article 34, 1. Indeed, this Article mentions the possibility of: "any actual or foreseeable negative effects on civic discourse and electoral processes, and public security" ((c)), and how, among other factors, their moderation content or advertising/recommendation systems play a part in the development of those risks (Article 34, 2.). Lastly, Article 35 requires that the providers "shall put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified under Article 34, with particular consideration to the impacts of such measures on fundamental rights".

The designation of the competent authorities in the DSA is provided by Article 56. In substance, it follows a principle very well known by French administrative jurists: "la compétence suit le fond", meaning that the designation of an entity as competent is the result of the nature of the law applicable. Indeed, when the common block of requirements is at stake, the competence is attributed in principle to the national authorities; on the other hand, the enforcement of the enhanced block of requirements calls intervention of the EC, without exception. To better understand the designation of the competence, the following precisions must be mentioned. Indeed, Article 56, par. 2, gives a pre-emption power to the EC to enforce the common block of requirements against very large enterprises, the national authorities hence finding a subsidiary competence precised by par. 3. They will be allowed to enforce the common block against very large enterprises only "where the EC has not initiated proceedings for the [infringement of the common block]". This distinction is consistent with the principle of subsidiarity.

In the surveillance of the very large providers, the EC beneficiates from the active participation of these actors. Indeed, as mentioned before, the DSA calls the very large providers to notify the EC of possible risks, to conduct audits, and to pay an annual fee to the EC to "compensate" for the surveillance costs. Hence, these obligations allow the EC to receive an amount of information without having to conduct an enquiry. However, if the necessity of leading one was to be raised, the EC wouldn't be impotent. Indeed, the EC can request documents (Article 67), organise interviews and gather declarations (Article 68), and power to conduct inspections (article 69). Even more, the EC have the power to sanction the infringement. Overall, the similarities between the powers granted to the national authorities and the EC in matters of competition law are here blatant.
In addition to the sanction powers, the EC has an important role to play through crisis handling, and report duty. Under the wording of Article 34, 2.: "a crisis shall be deemed to have occurred where extraordinary circumstances lead to a serious threat to public security or public health in the Union or in significant parts of it". Article 36 authorises the EC to require very large service providers to adopt specific measures, conceived with respect to the proportionality principle (Article 36, 1., (b)), to solve the threats at the roots of the crisis.
If this urgency power can be saluted, it has to be highlighted that this power is under a territoriality clause for its activation. Indeed, for a crisis to activate this Article, and besides the requirement related to the threat's intensity, it has to be over the whole EU, "or in significant parts of it". Hence, it seems plausible that the EC won't see its competence recognised when a threat is limited over the territory of only one MS, or few. This may cause a problem to the extent that, under Article 56 which organises the distribution of competence to enforce this directive, MS's authorities don't have any competence to enforce Chapter III, section 5, even in the absence of EC actions. Hence, MSs would have to go further than the DSA's frameworks to be able to act against such threats, in a tight window. Indeed, MS would have to demonstrate the existence of a local crisis justifying the action of MS's authorities, in the absence of EC's action under Article 36, 70 (interim remedies) or 73 (infraction decision), that justify for it to pronounce measures such the ones granted to the EC by article 36. It is to be expected that, in such a situation, a very large service provided under the empire of such national measures would want the national judge to address a preliminary question to the CJEU, to contest the competence of the State to adopt such act.
Lastly, the EC is, according to Article 35(2), under the obligation to publish an annual report on the most important and frequent risks encountered, and the best practices to mitigate them, at the national level principally.

For the first time, the EC launch an official investigation on December 18, 2023, against *X* (formerly "*Twitter"*). Among other point, the EC will focus on the propagation of illegal content and the way *X* addresses information manipulation[118].

To sum up, the DSA provides an obligation to the companies providing online platforms or research engines used by a large fraction of EU citizens to be more transparent and responsible for the content they provide to their users. The goal here is to avoid that, by using these platforms, foreign entities spread disinformation to EU citizens. Indeed, mass disinformation by foreign entities is seen as a threat to national security by the EP. To pursue that aim, EU legislators are working on a proposal for the EC, to regulate online political advertisement. This is the subject of the next part.

3.2. Political advertising, a more specific regulation to avoid foreign influence

The Proposal for a regulation of the EP of the Council[119] *on the transparency and targeting of political advertising*, is an incoming secondary legislation. It has for purpose to bring a precise answer to the threats caused by FIMI to the democratic processes within the EU, and to harmonise this sector as discrepancy have been constated within MSs' legislations[120]. Its legislative procedure is still ongoing, with the peculiarity that, after the first reading, it has been referred to the responsible committee for interinstitutional negotiations[121]. This first reading before the EP brought considerable adjustments to the proposal, to the benefits of the EU institutions that find now reinforce role. Hence, for the purposes of this demonstration, the amended version of this

[118] European Commission - European Commission. « Commission Opens Formal Proceedings against X under the DSA ». Press release. Conculted on December 31, 2023. https://ec.europa.eu/commission/presscorner/detail/en/IP_23_6709.
[119] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the transparency and targeting of political advertising (2021). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0731.
[120] *Ibidem*, part: "Reasons for and objectives of the proposal"
[121] « 2021/0381(COD) - 02/02/2023 - Transparency and targeting of political advertising ». consulted on December 14, 2023. https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1732680&t=e&l=en.

proposal will be analysed, available on the *Legislative observatory* website of the European Parliament[122].

This Regulation proposal carries, in a similar way as the DSA, the obligation related to the transparency, to the framing, and to the control of advertising of service online platforms. However, its obligations are tailored to address to the sensitiveness of political advertising. The cooperation between the two regulations is solved by this Proposal's Article 2, which provides that the definition of political advertising services should be used in first, with a requalification as an intermediary services provider when those are not involved with the message carried by their services. Indeed, article 2, par. 5 provides that political advertising services: "*means a service consisting of political advertising with the exception of an online intermediary service within the meaning of Article 2(f) of Regulation (EU) 2021/XXX [Digital Services Act] that is provided without consideration for the placement, publication or dissemination for the specific message"*[123]. In other words, for a provider to not be under this proposal 's scope of application, it must remain neutral toward the message "broadcasted".

For the author, this regulation finally addresses a risk well-known by European legislators since the Cambridge Analytica case. This risk is the following: with targeted processing of data, it is possible to influence pools of voters, and, logically, if the sponsor of such influence is a foreign influence, it can threaten national security is certain. To mitigate this risk, the regulation provides political advertisement publishers with the obligation to ensure sufficient labelling of political advertising. To that end, the amended proposal indicates at its Article 7 a list of three mandatory labels. First, must be presented as an indication that it is a political advertisement; second, must identify the identity of this advertisement's sponsor, or its controlling entity; third, must be given a transparency notice, or a link to that notice, informing on the wider context of the political advertisement. To enforce this Article, the EP enforced the EC with a power, provided by a new Article 7, 1), b., to adopt a delegated act standardising the labelling technique, with respect to the "latest technological and market developments, relevant scientific research and best practices."

---

[122] https://www.europarl.europa.eu/doceo/document/TA-9-2023-0027_EN.html

[123] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the transparency and targeting of political advertising (2021). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0731.

This proposal also gives specific rules for data processing undertaken for political advertising purposes.

Those rules are to be viewed as a lex specialis to the rules laid down in the GDPR. They frame further the processing of certain categories of data to avoid too much precision in the targeting. Indeed, Amendment 112 provides: "[Article 1] 4a. The data protection rules on processing of personal data provided for in this Regulation shall be considered as specific data protection rules to the general rules laid down in the Regulations (EU) 2016/679 and (EU) 2018/1725". Thus, Article 12 provides with "Specific requirements related to the processing of personal data for online targeting and ad delivery techniques" (amendment 203). Firstly, in the continuity of Article 9 GDPR, Article 12 prohibits the processing of sensitive data; for the other types of data, and "in the context of political advertising services [data processing] shall be strictly limited to the situations provided for in this Article". With this 204th amendment, the EP goes much further than the original Article 12 by introducing stricter rules to data processing than the GDPR, a specific regime in the context of political campaigns. This modification is to be seen as particularly welcomed. Indeed, the data processing denounced in the Brexit referendum, or the US presidential elections of 2016, wasn't dependent on sensitive data to identify influenceable voters. Overall, these rules will mitigate the precision of political advertisement targeting, however, one of the main inputs of this regulation is the obligation, for the data controller to collect the data subject's specific consent to have its data processed for the unique purpose of online political advertising (Amendment 207). This requirement should first raise the awareness of the user on the ends their data are used for, in raising the user's attention on this specific point. The EP also went with further precision to limit the precision of data processing techniques. Indeed, the same amendment limits 3 the number of data categories of data that can be used, in addition to data location, in targeting and delivering advertising. Even more, the precision of data location is strongly restricted to the level of the constituency relevant at the time of the election, to the municipality level in the absence of such context.

Overall, in the author's opinion the DSA, and this Proposal with even more efficiency, will bring a massive change in the office of the national authorities in charge of analysing the regularity of elections. Indeed, such rules will be added to the relevant corpus of legislation that, for example, the French Conseil Constitutionnel could have in the future the duty to the questions related to the regularity of an election or a vote. It also questions the question of subsidiarity of the enforcement.

Indeed, on a question with such importance as one of the national elections, it is possible to question the true legitimacy of EU's institutions to enquiry and to "relieve the national data protection authority or authorities, or any competent authority where applicable, of its powers regarding the infringement at stake to supervise and enforce the obligations under this Regulation" when investigating against a VLOP or VLOSE (amendment 226). Indeed, it would lead in such circumstances to the deprivation of a national judge, in the case of the French legal order: a Constitutional Court, of the role of controlling the most important election of a country. It might be viewed by some as an unbearable infraction in MS's sovereignty.

Lastly, this amended regulation provides for an enhanced role of the EU citizens, through an enhanced notification mechanism and a right to effective remedies. Indeed, this proposal suggests a special notification system (article 9 amended), and its amended version provides for a right to complain (Amendment 245). The notification system provides that the notification mechanisms must be efficient by being, notably, user-friendly and allowing for the most precise notification; the user must also be granted feedback on their notification. Amendment 186 brings a new requirement, the obligation of the political advertisement publisher to deliver an answer within a timeframe of 48 hours after the notification period of elections. The same, shortened, obligation of responses is provided for the information requests of authorities (Proposal's Article 10), or other interested entities within the meaning of Article 11 of the proposal.

Furthermore, the amended version of the proposal provides for a right for individuals and legal persons to lodge a complaint before the competent authority (Amendment 246). Once again, it shows how the EU institutions relies on the complementarity between public and private enforcement — that emerged formally with recent cases-law of competition law[124], but that is, in fact, an essential characteristic of UE law identified as soon as in *Van Gend & Loos*[125], with the affirmation of the MS's judges' roles of 1st instance judges —, to enforce its law.

[124] Vantaan kaupunki v Skanska Industrial Solutions Oy and Others, No. Case C-724/17 (ECJ 14 mars 2019), par. 45.
[125] NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration, No. Case 26-62 (ECJ 5 février 1963).

3.3. Summary

This part tends to demonstrate, based on the idea that foreign influence on democratic processes is a threat to national security, the legislative initiative from the EU to fight against this threat. Firstly, with the DSA, the EU provides obligations to the providers of large online services to share information with their users on the way content is suggested to them. To do so, they must give information on how their algorithms work, and make available to the user that a given content is an advertisement. This has the purpose of making the EU citizens more aware of how the content they are seeing is chosen. By doing so, they can become more aware of the external influence that online services can have on them, and more aware of advertisement. This should decrease the efficiency of advertisements, especially when they are paid by foreign entities. Even more, the providers have the responsibility to fight against disinformation. The EP recognised the negative effect of disinformation of foreign influence and disinformation, especially on political processes, to the extent it qualified it as a threat to national security. Hence, on a proposal from the Commission, a regulation is in the legislative process. This regulation on online political advertisements will regulate further the content of online services. The purpose is to allow for more transparency of online political advertisements and to frame further the processing of data in that context. Indeed, to target this kind of advertisement, data controllers will have a limited number of categories of data, and they will be limited in the precision of the targeting. Here again, the purpose is to mitigate the effect of online advertisement on democratic processes and to avoid disinformation and foreign influence from affecting the results of the elections of EU territories.

CONCLUSIONS

1. The CJEU cases-law analysis demonstrates that both the initiatives from MSs and EU's legislator to initiate a European approach to limit personal data protection for national security are limited. Indeed, the CJEU adopts a very strict stance to protect human rights. This stance it's even more uncommon that the ECtHR, on the other hand, the human rights court by design, recognised to its Contracting Parties a large margin of appreciation. Hence, this side of the European approach to personal data protection and national security is of a praetorian nature. Its coherence is limited by the duality of its conception but ensured by the intertwining of the two legal orders that require the two-judge to adopt, most of the time, a conciliant posture, which manifests notably by a strong indirect dialogue constituted by numerous referrals to each other's case law within their own decision.
2. Under the principle of subsidiarity, the CJEU and the ECtHR frame the States under their jurisdiction in their will to exploit personal data for national security purposes. Both courts had to adapt their review to face the challenge of secrecy, which prevented them from having a deeper review of the situations of facts of the cases. Hence, the two courts provide in their case law a list of criteria for the States to follow. The spirit of the regime they drew is that the processing of personal data in secret, for purposes of national security, must be sufficiently framed in time and in the circumstances, they can be adopted to act on. The proportionality of the measures must be checked by national authorities, to develop an "end-to-end" control, from the adoption of the measures to its application, and its post-facto review.
3. The Council of Europe is less able to provide impetus to the European approach than the EU. Indeed, unlike the EU, the Council of Europe has not been given legislative or executive functions in certain areas; its only mode of action, when the need arises to legislate on new subjects, is through international convention, a tool that is far less flexible and effective to affect the legal situation of individuals. Because the ECtHR only acts a posteriori, and despite a case-law leaning to give solutions to be applied by the contracting parties at the gestation of their legislations, the Council of Europe finds difficulties to be a "motor", an impulsion to initiate a European approach. This is where the EU comes into its own: the direct effect of its law is recognized, and its legal system is perfected.

4. Against FIMI, a problematic area for the protection of national security, the EU is building secondary law to regulate the services provided online. The Digital Services Act provides for enhanced transparency and responsibilities from the service providers. The biggest providers are under the obligation to mitigate the systemic risks that their platform can nurture, risks that the EU legislator identified as able to cause risk to public security. Indeed, mass disinformation online, coupled with political advertising fomented by foreign actors can harm European democratic processes, for the final interest of foreign actors, which can, in fine, threaten national security. With the proposal for a regulation on online political advertisement, the EU pursue on the path to build a European approach to a protection of personal data that, notably, protection national security.

RECOMMENDATIONS

The author suggests the following recommendations:

1. For the EU to codify the case-law of *Quadrature du Net* within a directive to allow for a clarification of its regime that would benefit from the MSs' approval. Within it, an input would be to give the control of the national measures of surveillance to jurisdiction only, and not also to independent administrative authority, in order for this national jurisdiction to be able to make referrals to the CJEU.
2. To develop and codify the institution's bans, whether MS's or EU's, to companies that aren't complying with personal data protection law, when it threatens national securities, such as TikTok bans. Indeed, if such sanctions can justify, it can still constitute a violation to the principle of prohibition of arbitrary public interference in private activity, and judicial redress must be available to assess whether there is an arbitrary interference.
3. Concerning the next developments of the proposal for a Regulation of the EP and the Council *on the transparency and targeting of political advertising*. It is recommended to support the addition to this legislation of a provision requiring from the service provider to identify more clearly what content is proposed as a result of an algorithm's work. This addition, and even though some providers already implemented such feature, would ensure

users' awareness of the algorithms' results, and participate to mitigate the "echo chambers" effect.

LIST OF BIBLIOGRAPHY

Treaties:

1. Consolidated version of the Treaty on European Union (2016). http://data.europa.eu/eli/treaty/teu_2016/oj/eng.
2. Consolidated version of the Treaty on European Union, 326 OJ C § (2012). http://data.europa.eu/eli/treaty/teu_2012/oj/eng.
3. Charter of Fundamental Rights of the European Union, 326 OJ C § (2012). http://data.europa.eu/eli/treaty/char_2012/oj/eng.
4. European Convention on Human Rights, https://www.echr.coe.int/documents/d/echr/Convention_ENG

Legislation:

5. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance), 277 OJ L § (2022). http://data.europa.eu/eli/reg/2022/2065/oj/eng.

6. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the transparency and targeting of political advertising (2021). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0731.

7. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.), 295 OJ L § (2018). http://data.europa.eu/eli/reg/2018/1725/oj/eng.

8. Regulation (EU) 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) (Text with EEA relevance), 119 OJ L § (2016). http://data.europa.eu/eli/reg/2016/679/oj/eng.

9. Directive (EU) 2016/680 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 prosecution 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, 119 OJ L § (2016). http://data.europa.eu/eli/dir/2016/680/oj/eng.

10. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 201 OJ L § (2002). http://data.europa.eu/eli/dir/2002/58/oj/eng.

11. 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, 281 OJ L § (1995). http://data.europa.eu/eli/dir/1995/46/oj/eng.

Official documents:

12. European Parliament resolution of 1 June 2023 on foreign interference in all democratic processes in the European Union, including disinformation (2022/2075(INI)) (2023). http://data.europa.eu/eli/C/2023/1226/oj/eng.

13. ENISA. « ENISA Threat Landscape 2023 ». Report/Study. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

14. Sénat. « La tactique TikTok : opacité, addiction et ombres chinoises - Rapport ». Report. https://www.senat.fr/rap/r22-831-1/r22-831-1.html.

15. European Commission - European Commission. « Commission Opens Formal Proceedings against X under the DSA ». Press release. https://ec.europa.eu/commission/presscorner/detail/en/IP_23_6709.

Case-law:

CJEU:

16. Ligue des droits humains ASBL v Conseil des ministres, No. Case C-817/19 (ECJ 21 juin 2022).

17. GD v The Commissioner of the Garda Síochána and Others, No. Case C-140/20 (ECJ 5 avril 2022).

18. Proceedings brought by B, No. Case C-439/19 (ECJ 22 juin 2021).

19. Privacy International contre Secretary of State for Foreign and Commonwealth Affairs ea, No. Affaire C-623/17 (Cour de justice 6 octobre 2020).

20. La Quadrature du Net and Others v Premier ministre and Others, No. Joined Cases C-511/18, C-512/18, C-520/18 (ECJ 6 octobre 2020).

21. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, No. Case C-311/18 (ECJ 16 juillet 2020).

22. Vantaan kaupunki v Skanska Industrial Solutions Oy and Others, No. Case C-724/17 (ECJ 14 mars 2019).

23. Proceedings brought by Ministerio Fiscal, No. Case C-207/16 (ECJ 2 octobre 2018).

24. Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, No. Joined Cases C-203/15 and C-698/15 (ECJ 21 décembre 2016).

25. Maximillian Schrems v Data Protection Commissioner, No. Case C-362/14 (ECJ 6 octobre 2015).

26. Opinion of the Court (Grand Chamber) of 26 July 2017. Case Opinion 1/15. (ECJ 2015).

27. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, No. Joined Cases C-293/12 and C-594/12 (ECJ 8 avril 2014).

28. European Parliament v Council of the European Union (C-317/04) and Commission of the European Communities (C-318/04), No. Joined cases C-317/04 and C-318/04 (ECJ 30 mai 2006).

29. United Kingdom of Great Britain and Northern Ireland v Council of the European Union, No. Case C-84/94 (ECJ 12 novembre 1996).

30. Commission of the European Communities v Council of the European Union, No. Case C-122/94 (ECJ 29 février 1996).

31. Srl CILFIT and Lanificio di Gavardo SpA v Ministry of Health, No. Case 283/81 (ECJ 6 octobre 1982).

32. Amministrazione delle Finanze dello Stato v Simmenthal SpA, No. Case 106/77 (ECJ 9 mars 1978).

33. Opinion of the Court of 26 April 1977. Opinion 1/76. (ECJ 1976).

34. Procureur du Roi v Benoît and Gustave Dassonville, No. Case 8-74 (ECJ 11 juillet 1974).

35. NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration, No. Case 26-62 (ECJ 5 février 1963).

ECtHR:

36. Centrum För Rättvisa v. Sweden, No. 35252/08 (ECtHR [GC] 25 mai 2021).

37. Big Brother Watch and Others v. the United Kingdom, No. 58170/13, 62322/14, 24960/15 (ECtHR [GC] 25 mai 2021).

38. Roman Zakharov v. Russia, No. 47143/06 (ECtHR [GC] 4 décembre 2015).

39. Kennedy v. the United Kingdom, No. 26839/05 (ECtHR 18 mai 2010).

40. Liberty and Others v. the United Kingdom, No. 58243/00 (ECtHR 1 juillet 2008).

41. Broniowski v. Poland, No. 16153/09 (ECtHR [GC] 22 juin 2004).

42. Klass and Others v. Germany, No. 38581/16, 41914/16, 57510/16, 62644/16, 7190/17, 10973/17, 12530/17, 19411/17, 22087/17, 28475/17, 78165/17 (ECtHR 6 septembre 1978).

Scholar literature:

43. Alguliyev, Rasim M., Yadigar N. Imamverdiyev, Rasim Sh. Mahmudov, et Ramiz M. Aliguliyev. « Information security as a national security component ». *Information Security Journal: A Global Perspective* 30, nº 1 (janvier 2021): 1-18. https://doi.org/10.1080/19393555.2020.1795323.

44. Bignami, Francesca, et Giorgio Resta. « Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance ». SSRN Scholarly Paper. Rochester, NY, 2018. https://papers.ssrn.com/abstract=3043771.

45. Bouveresse, Aude. « Le pouvoir discrétionnaire dans l'ordre juridique communautaire ». Strasbourg 3, 2010.

46. Brkan, Maja. « The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors ». Maastricht Journal of European and Comparative Law 23, nº 5 (2016): 812-41.

47. Cors, Dylan. « National Security Data Access and Global Legitimacy Rule of Law ». Department of Justice Journal of Federal Law and Practice 67, nº 4 (2019): 257-86.

48. Dimitrova, Anna, et Maja Brkan. « Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts before and after the NSA Affair ». Journal of Common Market Studies 56, nº 4 (mai 2018): 751-67. https://doi.org/10.1111/jcms.12634.

49. Dupuy, Pierre-Marie, et Yann Kerbrat. *Droit international public*. 16e éd., 2022, Remaniée et Enrichie. Précis. Paris: Dalloz, 2022.

50. Hochen, Ru. « When Your Apps Threaten National Security - A Review of the TikTok and WeChat Bans and Government Actions under IEEPA and FIRRMA Symposium: A Life Navigating the Securities Markets: A Celebration of Professor Roberta Karmel's Work, Teaching, and Mentorship: Notes ». Brooklyn Journal of Corporate, Financial & Commercial Law 16, nº 1 (2022 2021): 193-224.

51. Gauthier, Catherine, Sébastien Platon, et David Szymczak. *Droit européen des droits de l'homme*. [Éd.] 2017. Université S. Paris: Sirey, 2016.

52. Lambert, Pierre, éd. *Les droits de l'homme au seuil du troisième millénaire: mélanges en hommage à Pierre Lambert*. Bruxelles: Bruylant, 2000.

53. Mata, Dan Constantin. « The Protection of Personal Data in the Context of National Security Protection Measures ». Revista Universul Juridic 2016 (2016): 144-48.

54. Morano-Foadi, Sonia, et Lucy Vickers, éd. *Fundamental rights in the EU: a matter for two courts*. Modern studies in European law. Oxford ; Portland, Oregon: Hart Publishing, 2015.

55. Oberg, Jacob. « The Definition of Criminal Sanctions in the EU ». European Criminal Law Review 3, nº 3 (2013): 273-99.

56. Perju, Vlad. « Reason and Authority in the European Court of Justice ». Virginia Journal of International Law 49, nº 2 (2009 2008): 307-78.

57. P. Pescatore, 2015, "The doctrine of "direct effect": an infant disease of Community Law", E.L. Rev. 2015, 40(2), 40(2), 135-153

58. Picod, Fabrice, Cécilia Rizcallah, et Sébastien Van Drooghenbroeck. *Charte des droits fondamentaux de l'Union Européenne: commentaire article par article*. 3e éd. Collection Droit de l'Union européenne 2. Bruxelles: Bruylant, 2023.

59. Renucci, Jean-François, et Antoine Renucci. *Droit et protection des données à caractère personnel: droit européen, RGPD, Convention européenne des droits de l'homme*. Manuel. Paris-La Défense: LGDJ, 2022.

60. Tambou, Olivia, et Juan Fernando López Aguilar. *Manuel de droit européen de la protection des données à caractère personnel*. Droit administratif, 28 28. Bruxelles: Bruylant, 2020.

61. Tinière, Romain, Claire Vial, et Frédéric Sudre. *Droit de l'Union européenne des droits fondamentaux*. Collection Droit de l'Union européenne 16. Bruxelles: Bruylant, 2023.

62. Tzanou, Maria, et Spyridoula Karyda. « Privacy International and Quadrature Du Net: One Step Forward Two Steps Back in the Data Retention Saga? » European Public Law 28, nº Issue 1 (1 février 2022): 123-54. https://doi.org/10.54648/EURO2022007.

63. Véron, Noémie. « Protection des données personnelles et renseignement: contribution à l'identification d'un régime juridique autonome ». Pau, 2022.

64. Walter, Jean-Philippe. « La Convention 108, un complément nécessaire à l'article 8 de la CEDH à l'heure du numérique ». *Civitas Europa* 49, nº 2 (2022): 251-61. https://doi.org/10.3917/civit.049.0253.

ABSTRACT

This master's thesis seeks to determine the substance of a European approach to personal data protection and national security. To do so, it investigates the sources of personal data law able to influence at a European scale: the Council of Europe and the European Union. As national security remains within the States' competencies, the first part consists of the study of the limitations that European States have to confront when acting for national security, and more precisely, the limitations made to defend personal data protection. In doing so, this research analyses and compares the case laws of the ECtHR and of the CJEU. Hence, if the first part of this master's thesis analyses the conflictual exchanges between national security and personal data protection, the second part analyses how the two concepts can be defended together. To do so, the second part focuses on the defence from foreign influence within democratic elections. Indeed, the link with the subject is that foreign influence on EU democratic processes can be realised by processing data of EU citizens, to influence them for the benefit of foreign entities. This processing of data tends notably to vastly disinform and target influenceable voters. The European Parliament called to act, qualifying it as a threat to "national security" in a resolution from June 1, 2023.

SUMMARY

Overall, it’s possible to distinguish two trends within the European approach to personal data protection and national security. The first is when the two notions are in contradiction, meaning that one is limiting the other, the approach is mainly praetorian. Indeed, as national security remains in MS’s sphere of competence the initiative can only come from the States, and the European approach consists in judges’ control of their initiative. The second is from the EU, which indirectly supports national security through enhanced personal data protection.

Within the Council of Europe, in parallel with the ECHR, the Parties gathered themselves around Convention 108, and Convention 108+ more recently. However, these two last instruments find limited enforceability within the national legal orders. Thus, the ECHR remains the more efficient tool, within the Council of Europe's legal order, to frame the restriction implemented by the States to the right to personal data protection, protected by Article 8. On the other side, the EU, through a dense aggregation of legislation, recognise national security as a basis to limit the fundamental right to personal data protection, as well as a motive to exclude the application of EU law. Indeed, Article 4 TEU recognises the exclusive competence of the MS to protect their national security. However, the CJEU, with its systematic and teleologic methods of interpretation, interpreted strictly the exclusion provision. Even more, the CJEU limits both initiatives from MSs and the EU’s legislators to initiate a European approach to limit personal data protection for national security. This strict stance it’s even more remarkable that the ECtHR on the other hand, the human rights protective court by nature, recognised a large margin of appreciation to the MS in that matter. Hence, it’s possible to qualify that the first side of the European approach to personal data protection and national security limitation is of praetorian nature. Its coherence is limited by the duality of its conception but ensured by the intertwining of the two legal orders. Hence, the European approach, in limiting the possibility for the MS to restrict the right to personal data protection for national security, is mainly the product of the judge’s controls.

When it comes to protection the of personal data for national security, the EU is the main motor. This master’s thesis identified the need to ensure that the companies processing the personal data of EU citizens don’t threaten MS’s national security. On this last point, it has been distinguished the peculiar case of FIMI. It led to the building of different secondary legislations, bringing the rule of law to digital services, which were for a long time under the exclusive supervision of private

companies. These kinds of “digital” far west are nowadays under the rules of the Digital Services Act which provides for enhanced transparency and responsibilities from the service providers, that are now under the obligation, for the biggest, to mitigate the systemic risks that their platform can nurture. Moreover, this regulation prolongated the innovation formalised in competition law which consists of emphasizing the complementarity between private and public enforcement of EU law. Furthermore, this recipe will also be present in the, to be delivered, as it is hoped by the author, regulation on the transparency and targeting of political advertising. This regulation will further limit the use of personal data for purposes of political advertising. Indeed, it will restrict the geographical precision and categories of personal data that can be used to four, as well as require the data controller to require the data subject to give consent for its data to be used for political advertisement purposes.