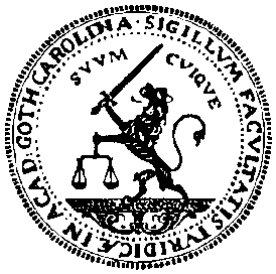

FACULTY OF LAW

LUND UNIVERSITY

Alise Forsman

Data Protection and the Division of Legislative Power

Enforcement of the EU Fundamental Right to Protection of Personal Data after Case C-817/19 *Ligue des droits humains*

JURM02 Graduate thesis

Graduate Thesis, Master of Laws program

30 higher education credits

Supervisor: Professor Xavier Groussot

Semester: HT 2022

Contents

Summary

This thesis centers data protection as a constitutional right in the EU, as enshrined in Articles 7 and 8 of the Charter of Fundamental Rights, and examines the circumstances under which the right can be limited. Regulation of the use of personal data as a legislative field in the EU has clear ties to human rights, economic and market interests, and interests of law enforcement and national security. With the development of new technology such as predictive modelling, data protection is becoming increasingly important.

The Court of Justice has tended to give data protection a strong stance in its jurisprudence. On 21 June 2022 the Court handed down another landmark judgement on data protection, Case C-817/19 *Ligue des droits humains*, in which it chose not to invalidate the PNR Directive although it entailed serious interferences with the right to data protection. In its judgement, the Court upheld a general principle of interpretation, namely that an EU act must be interpreted, as far as possible, in such a way as not to affect its validity. The interferences of the PNR Directive were found to be proportionate to the objective of combatting terrorist offences and serious crime.

In this thesis is examined how data protection is upheld as a fundamental right in the context of national security by analyzing the judgement of *Ligue des droits humains*. The implications of the judgement are considered in relation to the concepts of essence, proportionality, and necessity.

The thesis argues that the application of the general principle of interpretation led the Court to limit the extent of its judicial review, the appropriateness of which can be questioned in a case with such strong ties to fundamental rights. Seemingly the Court imposes on itself an obligation to limit the right to data protection to a minimum, or to its essence. Although the Court circumvented taking a clear stance on the *stricto sensu* proportionality of the interference in its analysis, in conclusion, the fundamental right to data protection was outbalanced by the interest of national security.

In its efforts not to invalidate the PNR Directive, but at the same time keep it limited to what is strictly necessary, the Court allowed itself a wide margin of interpretation to adjust its provisions. Such interpretations create friction between the law as made by the Court in its judgement and the law as crafted by the EU legislature, which subverts the division of powers between the judicial and legislative bodies of the EU. How well Member States will follow the amendments to the PNR Directive as made by the Court, and its potential implications on future legislation regulating the use of PNR data remains to be seen. After *Ligue des droits humains*, the CJEU has strengthened its own mandate to co-legislate together with the EU legislator.

Sammanfattning

I denna uppsats undersöks dataskydd som en konstitutionell rättighet i EU och de omständigheter under vilka rättigheten kan begränsas. Rätten till respekt för privatlivet och skydd för personuppgifter återfinns i artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Regleringen av användningen av personuppgifter är ett lagstiftningsområde i EU av växande betydelse, med tydliga kopplingar till mänskliga rättigheter, ekonomiska och marknadsintressen samt brottsbekämpning och nationell säkerhet. I takt med utvecklingen av ny teknik såsom artificiell intelligens blir rätten till dataskydd allt viktigare.

EU-domstolen har tenderat att ge skyddet för personuppgifter en stark ställning i sin praxis. Den 21 juni 2022 gick domstolen emot denna trend i mål C-817/19 *Ligue des droits humains*, när den valde att inte ogiltigförklara PNR-direktivet trots att det innebar betydande ingrepp i rättigheterna som garanteras i artiklarna 7 och 8 i Stadgan. I sin dom tillämpade domstolen allmänna tolkningsprinciper som innebär att en unionsrättsakt ska tolkas, så långt möjligt, på ett sätt så att dess giltighet inte påverkas. De ingrepp som PNR-direktivet innefattade befanns stå i proportion till sitt syfte, att bekämpa terroristbrott och grov brottslighet.

I uppsatsen undersöks hur den grundläggande rätten till dataskydd balanseras gentemot nationell säkerhet genom att analysera *Ligue des droits humains*. Följderna av domen övervägs i relation till begreppen rättighetens väsentliga innehåll (essens), proportionalitet och nödvändighet.

Tillämpningen av de allmänna tolkningsprinciperna ledde till att domstolen begränsade omfattningen av sin konstitutionella domstolsprövning. Lämpligheten av detta ifrågasätts utifrån den starka anknytningen i målet till grundläggande rättigheter eftersom EU-domstolen på så sätt ålägger sig själv en skyldighet att begränsa rätten till dataskydd så långt som möjligt. I sina ansträngningar att inte ogiltigförklara PNR-direktivet, men samtidigt hålla det begränsat till vad som är strikt nödvändigt, tillät domstolen sig ett stort tolkningsutrymme för att justera direktivets bestämmelser. Sådana justeringar av direktivet skapar dissonans mellan gällande rätt, så som den uttolkats av domstolen och så som den föreskrivits av lagstiftaren, vilket undergräver maktfördelningen mellan EU:s dömande och lagstiftande organ. Hur väl medlemsstaterna kommer att införliva de tolkningar som gjorts i *Ligue des droits humains*, och domens potentiella inverkan på kommande dataskyddslagstiftning återstår att se. I domen undvek EU-domstolen att tydligt ta ställning vad gäller proportionalitetsavvägningen mellan de motstående intressena, men slutsatsen kan dras trots detta är att intresset av att upprätthålla nationell säkerhet vägde tyngre än den grundläggande rätten till dataskydd.

Preface

Ett varmt tack till min handledare Xavier Groussot som gjort denna uppsats många gånger bättre och enklare att skriva. Jag vill även tacka familj och vänner som hjälpt mig med gott lunchsällskap, pepp, råd och korrekturläsning. För att avsluta min studietid, och inleda denna uppsats, har jag tagit mig friheten att låta min inre poet få publicera en dikt med reflektioner över något av vad jag lärt mig under min tid på juristprogrammet. Resultatet av det ser du nedan. Slutligen, till dig som ska läsa önskar jag mycket nöje.

Alise Forsman
Malmö den 4 januari 2023

[Law]

To put in its place.

[Lawyer]

Someone who puts in its place.

Law is the never-ending strive
to understand the world, and organize,
its every detail into structure.

There is no thing, place, item, person,
event, act, relationship, or occurrence
that cannot be put in its place.

Anything you can look at
has been touched, with power
to possess and shape, by the Law.

Its appeal lies exactly there.

The will and creativity
the world demands to be understood
is nothing but inspirational.

But the Lawyer cannot afford
to never see chaos, the world
unregulated, if you like, raw.

The world can also be,
without, the law that governs it
which We must never forget.

Abbreviations

the Charter	Charter of Fundamental Rights of the European Union
CJEU / the Court	Court of Justice of the European Union
CoE	Council of Europe
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EU	European Union
GDPR	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) [2016] OJ L119/1
Ligue des droits humains	Judgement of 21 June 2022, Ligue des droits humains, C-817/19, EU:C:2022:491.
PIU	Passenger Information Unit
PNR	Passenger Name Record
PNR Directive	Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJ L 119/132.
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
U.S.	United States of America

1 Introduction

1.1 Background

With the development of new technology, data protection is becoming increasingly important. Or, by the expression of the Commission, Council, and European Economic and Social Committee of the Region in *a European strategy for data*:

> In a society where individuals will generate ever increasing amounts of data, the way in which the data are collected and used must place the interests of the individual first, in accordance with European values, fundamental rights and rules.[1]

In the strategy it is further proclaimed that "[d]ata is the lifeblood of economic development", "[d]ata will reshape the way we produce, consume and live" and "[b]enefits will be felt in every single aspect of our lives".[2] Without a doubt data and its uses are highly regarded as an extremely important legislative field in the eyes of the EU legislature.

As a first point of departure, it is necessary to clarify the role of technology in this legal context. This thesis revolves around the usage of personal data, in other words: information about a living, identifiable natural person.[3] In recent years, it has become easy and cheap to access, collect, store, edit, and systemize large amounts of data about a person that can derive from different times and places.[4] This increase in data and its availability is sometimes referred to in terms of 'big data'. Using predictive modelling that can be self-learning, knowledge is produced simultaneously as it is extracted, contributing to the flexibility and exponential increase of available data.[5]

In combination with other types of knowledge, such as social science and behavioral science, predictive modelling creates the potential to manipulate human behavior.[6] As proclaimed by Zuboff, behavior has become a commodity.[7] The rise of technology in a neoliberal society, she argues,

[1] European Commission, "Communication from the Commission to the Euro-pean Parliament, the Council, the European Economic and Social Committee of the Regions, *A European strategy for data*" COM (2020) 66 final, 1.

[2] European Commission (not 1), 2.

[3] Article 4(1) GDPR provides a description of the term as used in the EU legal system.

[4] Lebeck, C. (2016). *EU-stadgan om grundläggande rättigheter* (2., [rev.] uppl.). Studentlitteratur, 279.

[5] Greenstein, S. (2017). *Our humanity exposed : predictive modelling in a legal context.* Department of Law, Stockholm University, 79 & 122–123.

[6] Greenstein (not 5), 431.

[7] Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs (The Hatchett Group), 100.

institutes a form of surveillance capitalism that threatens democracy.[8] As a phenomenon, processing of personal data poses great perils to the rights and freedoms of individuals, but at the same time is essential for the functioning of society, not to mention desirable for the benefits it offers. The use of predictive models is undisputedly in general extremely beneficial to society.[9]

This has given rise to a legal context in which the 'network society' or 'data-driven economy' needs to balance multiple interests. The free flow of personal data is important for the functioning of the EU internal market and thus one of the main objectives of data protection legislation alongside individual rights.[10] Or as legal scholar Lynskey puts it, the EU data protection regime is a hybrid instrument that serves dual objectives.[11] In the EU, the first major data protection legislation was the Data Protection Directive[12], adopted in 1995. Since then, the EU data protection regime has expanded and will continue to do so over the coming years.[13] The role of the EU Charter of Fundamental Rights[14] (the Charter) in this context, specifically Articles 7 and 8, impose data protection as a fundamental right on primary level. As such the right has priority in case of conflict with rules laid out in secondary law.[15] The Charter creates the baseline of protection for individuals as they come in contact with technology. It is therefore essential to examine how the right to protection of personal data is enforced.

1.2 Research Question

This thesis centers data protection as a constitutional right in the EU and takes on a human rights perspective. Data protection as a legislative field in the EU is an area of growing importance to a multitude of interests and actors to consider. It has clear ties to human rights, economic and market interests, as well as interests of law enforcement and national security. It is therefore a particularly complex and pressurized context in which the role of human rights and the conditions under which these are limited are pushed to their limits.

---

[8] Zuboff (not 7). 8–12.

[9] Greenstein (not 5), 431.

[10] See i.e. Recital 2 GDPR.

[11] Lynskey, O. (2015). *The foundations of EU data protection law (1st edition.).* Oxford University Press, 132.

[12] 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 [1995] OJ L281/31.

[13] The EU legislature is currently working to update and create new acts, i.e., the e-Privacy Directive that is expected to be replaced by a regulation, the Data Governance Act (published on 3 June 2022, applicable from 24 September 2023), the Digital Services Act (adopted on 5 July 2022), the Digital Markets Act (adopted on 18 July 2022), the AI Act (proposal published on 21 April 2021).

[14] Charter of Fundamental Rights of the European Union [2012] OJ L326/391.

[15] See Chapter 1.3.1 below.

The Court of Justice of the European Union (CJEU) has given the fundamental rights to privacy and protection of personal data, as enshrined in Articles 7 and 8 of the Charter, a strong stance through its case law and invalidated several provisions for interference with the rights.[16] In its judgement of 21 June 2022 *Ligue des droits humains*[17] the CJEU went against this trend. The Court found that the PNR Directive[18] entailed "undeniably serious interferences with the rights guaranteed in Articles 7 and 8 of the Charter".[19] Still the Court did not declare the directive invalid but rather found its interferences to be proportional to the objective of safeguarding national security, an objective of "paramount interest".[20] By analyzing the jurisprudence of the CJEU, mainly *Ligue des droits humains*, this thesis aims to examine how data protection as a fundamental right and the interests of individuals it aims to safeguard, are balanced in situations where secondary law interferes with the rights in the Charter. To achieve this purpose the following questions, one central and four subsidiary, will be answered.

How is the fundamental right to data protection enforced?

- How does the right to protection of personal data, as enshrined in the Charter, influence secondary EU data protection law?
- Under what circumstances can the right to protection of personal data be limited?
- How are the concepts of essence, proportionality, and necessity used when the CJEU balances the rights guaranteed in the Charter against other interests?
- Has the enforcement of the right to protection of personal data changed after *Ligue des droits humains*? If so, how?

1.3 Methods and Material

This thesis uses a legal doctrinal method to analyze data protection on a constitutional level in the EU legal system, with a focus on its enforcement and how it affects the legality of secondary law. Legal doctrinal method is aimed at describing and understanding existing law (*de lege lata*) and at searching for practical solutions or the best outcome that is compatible with

[16] See Chapter 2.1 below.

[17] Judgement of 21 June 2022, Ligue des droits humains, C-817/19, EU:C:2022:491.

[18] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJ L 119/132.

[19] Ligue des droits humains (not 17), para 111.

[20] Ligue des droits humains (not 17), para 170 & 228.

the existing legal system (*de lege ferenda*).[21] This thesis is organized around the description and systemization of data protection as a fundamental right, *de lege lata*. A *de lege ferenda* approach is adopted as the judgement of the CJEU in *Ligue des droits humains* is analyzed from the perspective of examining how well the judgement and its implications 'fits' with the existing legal system.

Legal research is at its core goal oriented and aims to resolve conflicts that appear in legal systems.[22] The understanding of law as exactly that, a system, is one of the defining traits of the doctrinal approach since it requires the systemization and organization of legal sources.[23] EU legal method centers the EU legal system as an autonomous legal order characterized by its division into two levels – the supranational and national levels.[24] Since this thesis does not examine the implications of *Ligue des droits humains* on a national level, its main focus is on the supranational level.

The CJEU is the judiciary power and only institution of the EU with the authority to bindingly interpret EU legal acts.[25] Jurisprudence from the Court is therefore one of the most important legal sources of the EU legal system,[26] and of this thesis, together with the provisions of the Charter and relevant EU law. Further, this thesis uses sources that are not recognized in the EU legal hierarchy, such as guidelines from the EDPS and communications from EU institutions. The literature referred consists of peer reviewed academic texts which therefore are considered reliable as sources of information. Lynskeys book *The foundations of EU data protection law*[27] has been of great relevance as well as Dalla Cortes analysis of proportionality in the CJEU's data protection jurisprudence.[28]

1.3.1 The EU Legal System

The EU legal system is based on the rule of law which is reflected in Article 2 TEU. Its legal sources are divided into primary law, which is of a higher authority, and secondary law. Legal research on fundamental rights requires

[21] Smits, J. M. (2017), "What is legal doctrine?: On the aims and methods of legal-dogmatic research." in Van Gestel, R., Micklitz, H.-W., & Rubin, E. L. (eds.). *Rethinking legal scholarship: A transatlantic dialogue.* Cambridge University Press, 213.

[22] Åhman, K. (2019). *Grundläggande rättigheter och juridisk metod : RF 2 kap., Europakonventionen och EU:s stadga och deras tillämpning (Andra upplagan).* Norstedts juridik, 24–25.

[23] Smits (not 21), 211, 217–219.

[24] Reichel, J. (2018) "EU-rättslig metod." in Nääv, M. & Zamboni, M. (eds.). *Juridisk metodlära (Andra upplagan).* Studentlitteratur, 109.

[25] Article 19(1) TEU.

[26] Bernitz, U., & Kjellgren, A. (2022). *Europarättens grunder (Sjunde upplagan)*. Norstedts juridik, 61.

[27] Lynskey (not 11).

[28] Dalla Corte, L. (2022). On proportionality in the data protection jurisprudence of the CJEU. *International Data Privacy Law*, 12(4), 259–275.

specific attention to norm hierarchy since fundamental rights are recognized as superior to other legal sources. Based on Article 6 TEU, the Charter has the same legal value as the Treaties. There is no division of hierarchy within primary law, the Treaties and the Charter need therefore to be interpreted jointly.[29]

Fundamental rights are either qualified or absolute. Unlike absolute rights to which no exemptions are tolerated, qualified rights can be limited if the limitation is justifiable subject to the principle of proportionality.[30] Secondary law lacks the hierarchal status to limit fundamental rights but can nonetheless limit the extent of their protection and realization by means of the "textual hooks that allow a fundamental right to be limited by sub-constitutional law".[31] The textual hook in question, Article 52 of the Charter, allows secondary law to limit the rights set out in the Charter such as the right to data protection. The CJEU has the competence equivalent to that of a constitutional court to review the conformity of secondary law to its primary counterpart.[32] Secondary law that interferes with fundamental rights can therefore be invalidated by the CJEU if a fundamental right has been limited by the legislature to an unlawful extent. Regarding the Charter itself, the Court may not rule on the validity of primary law, only its interpretation.[33]

Through its jurisprudence, the CJEU has defined general principles of law such as the principle of proportionality, non-discrimination, and primacy under which EU law has priority before national legislation including national constitutions. The Court has typically derived these general principles from the provisions of the Treaties and the constitutional traditions of the Member States. As such, the principles are generally recognized as primary law and therefore have priority over secondary law.[34] Aside from being enshrined in the Charter, fundamental rights have 'primary law status' as general principles deriving from the constitutional traditions of the Member states and the ECHR.[35] With regard to the division of powers between the judicial and legislative powers of the EU, the Court may test the legality but not the expediency of an act.[36] Subject to the principle of proportionality, however, an act interfering with a fundamental right might be found unlawful if it is not suitable or necessary to achieve its goal.[37] The proportionality analysis thus "subverts any separation of powers scheme that holds that the Courts are prohibited from reviewing how a legislature has balanced among contending

[29] Åhman (not 22), 108.

[30] Stone Sweet, A., & Mathews, J. (2019). *Proportionality Balancing and Constitutional Governance : A Comparative and Global Approach*. Oxford University Press, 35.

[31] Dalla Corte (not 28), 5.

[32] Article 263 TFEU.

[33] Articles 264 & 267 TFEU.

[34] Bernitz & Kjellgren (not 26), 143–144.

[35] See Article 6 TEU and Chapter 1.3.2 below.

[36] Judgment of 12 November 1996, United Kingdom v Council, Case C-84/94, EU:C:1996:431, para 23.

[37] See Chapter 3.4.4. below.

social interests".[38] When reviewing an acts potential interference with a fundamental right, the Court is, on the one hand, restricted from interfering with the political choices made by the legislature in imposing the limitation of a fundamental right in favor of another interests. On the other hand, the proportionality analysis requires the Court to review and value such choices.

1.3.2 ECHR, Convention 108 & the Council of Europe

Parallel to the EU legal system exists the Council of Europe (CoE) which is an international law institute, holding two instruments with relevance to data protection: the ECHR and Convention 108. All EU Member States have ratified both conventions.[39] Regarding data protection, the two legal regimes have broadly similar aim with one notable difference. Data protection in the EU is largely tied to internal market functions whereas the CoE at its core is concerned with human rights.[40]

Article 52(3) of the Charter states that the meaning and scope of the rights in the Charter shall at least be the same as those in the ECHR, although the Charter may provide more extensive protection. For assessments of the Charter, interpretations made by the ECtHR of the ECHR are therefore of relevance, although not explicitly referred by the former.[41] Being an older instrument, the 1950 ECHR does not explicitly guarantee a right to data protection. The ECtHR has nonetheless extensively interpreted Article 8 ECHR, which recognizes the right to respect for private and family life, to include a right to protection of personal data.[42] The content of Article 8 ECHR therefore materially relates to that of both Articles 7 and 8 of the Charter. The protection provided for in those Articles should accordingly be at least equivalent to that provided for in Article 8 ECHR.

The ECHR is not the only CoE instrument that safeguards data protection rights. In 1981 the CoE adopted Convention 108 which recognizes the right to protection of personal data as a right on its own, separate from the right to

[38] Stone Sweet & Mathews (not 30), 37–38.

[39] Council of Europe, "Treaty Office; Full list – *Chart of signatures and ratifications of Treaty 005"* <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=005>; "Data Protection; Convention 108 and Protocols; Parties – *Convention 108 in the World"* <https://www.coe.int/en/web/data-protection/convention108/parties> accessed 2 December 2022.

[40] Bygrave, Lee A. (2021) The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects. *Computer Law & Security Review*, 40(April 2021, 105460), 7.

[41] Groussot, X., & Petursson, G. T. (2022). Je t'Aime... Moi Non plus: Ten Years of Application of the EU Charter of Fundamental Rights. *Common Market Law Review*, 59(1), 239–258, 252.

[42] See i.e. Amann v. Switzerland [GC], App no 27798/95, ECHR 2000-II; Rotaru v. Romania [GC], App no 28341/95, ECHR 2000-V.

respect for private and family life. There is no legal obligation to interpret EU law in line with Convention 108, as is the case with the ECHR. The contents of data protection legislation provided for by the CoE and the EU, however, mostly correspond and have to some extent developed symbiotically.[43] The courts that oversee the implementation of the ECHR and Convention 108 (ECtHR), and the Charter (CJEU) respectively, are independent courts of two separate legal systems, but tend to stay updated of one another's judgments and practice "mutual trust".[44] This further contributes to the overlap of data protection rights in Europe as upheld by the legal systems separately.

1.4 Delimitations

This thesis is delimited mainly by its material, *Ligue des droits humains* and the features of data protection that are relevant to the case, i.e. data protection in the context of national security. Being strictly occupied with data protection as a fundamental right, other aspects of data protection such as economic or market aspects, will therefore not be covered. The concepts of essence, proportionality, and necessity have been chosen as central because of their particular relevance to the judgement. Human rights and fundamental rights such as the right to private life and data protection are protected in Europe both by both by the CoE conventions and the EU Charter. This thesis has shortly taken notice of the interrelation between the two legal systems but will from here on focus mainly on the EU legal system.

1.5 Disposition

Above I have accounted for the legal and societal context in which the CJEU handed down its judgement *Ligue des droits humains*. In Chapter 2 I will describe how the fundamental right to protection of personal data, as enshrined in the Charter, has influenced secondary EU data protection law by looking at the jurisprudence of the CJEU, including the main case of this thesis *Ligue des droits humains*. Chapter 3 centers the right to data protection as a constitutional EU right and presents its core traits, how it has emerged in the praxis of the CJEU, and how it has been understood by legal scholars. The circumstances under which the can be limited are accounted for in Chapter 4. In Chapter 5, I will discuss the implications of *Ligue des droits humains* in relation to the concepts of essence, proportionality, and necessity. The final chapter contains a summarizing discussion on the findings in this thesis and aims to provide a conclusion in relation to the overarching research question: How is the fundamental right to data protection enforced?

[43] In 2018 the Convention 108 underwent an update to "Convention 108 +", the same year as the GDPR entered into force. The provisions share many similarities.

[44] Bernitz & Kjellgren (not 26), 165–167.

2 Enforcement of the Charter by the CJEU

The Charter has played a major role in the enforcement of EU data protection law. Likewise, the fundamental right to data protection has been central to the enforcement of the Charter. In this Chapter I will present the main material for this thesis, *Ligue des droits humains*. To provide context, I will first introduce some of the most relevant previous case law of the CJEU.

2.1 A Data Protection Friendly Court of Justice

The right to data protection based on the Charter has been given a "consistently prominent role" by the CJEU in its jurisprudence – both in comparison to other Charter rights and in comparison to how the right has been applied on a national level.[45] Looking at reports from national courts of the Charter's influence, Articles 7 and 8 of the Charter were among the most invoked in some jurisdictions, while other reports showed that in some Member States the Charter right to data protection had not been referenced at all.[46] Being ununiformly applied on a national level, the right to data protection based on the Charter has led to the CJEU handing down some of its most attention-grabbing judgements enforcing the right on a constitutional level.

The first case where the CJEU partly invalidated legislation on the basis of interference with the Charter was in relation to articles 7 and 8 of the Charter in *Volker and Eifert*.[47] The first time an EU act in its entirety was invalidated on the basis of interference with the Charter was also in a data protection case, *Digital Rights Ireland*.[48] The directive that was invalidated was the Data Retention Directive[49] which obligated communication service providers to retain personal data for the purpose of the investigation, detection, and

[45] Lynskey, O., "Article 8: The Right to Data Protection." The EU Charter of Fundamental Rights in the Member States." in Bobek, M., & Prassl, J. (2020). *The EU charter of fundamental rights in the member states.* Hart Publishing, an imprint of Bloomsbury Pub, 354.

[46] Lynskey (not 45), 355. Invoked frequently in the UK, Austria, the Slovak Republic, France, and Italy. Not referenced at all in Bulgarian, Hungarian, and Polish reports.

[47] Judgement of 9 November 2010, Volker und Markus Schecke and Eifert v Land Hessen, C-92/09 and C-93/0, EU:C:2010:662.

[48] Judgement of 8 April 2014, Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238.

[49] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54.

prosecution of serious crime, giving national authorities access to the retained data.[50] The CJEU declared that in adopting the directive, "the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter".[51]

It was also in relation to data protection, in *Schrems I*, that the CJEU annulled an EU act on the basis of interference with the essence of a right for the first time.[52] In doing so the Court invalidated the Commissions EU-U.S. 'Safe Harbor' agreement regulating the transatlantic transfer of personal data in accordance with the GDPR.[53] The Court has continued to strike down international agreements in relation to transborder data flow and communication of personal data to third countries. In *Opinion 1/15* the Court concluded that an envisioned agreement between Canada and the EU allowing for the transfer of personal data about air passengers was incompatible with the Charter, particularly because it allowed the use and retention of sensitive data.[54] In *Schrems II* the Court invalidated the EU-U.S. 'Privacy Shield' agreement because of its interference with the Charter.[55] In doing so, specifically in the name of safeguarding fundamental rights, the CJEU exercised its power as a constitutional court extraterritorially and even aggressively.[56]

Any claim that data protection legislation is merely symbolic or simply functioning to uphold the 'status quo' has consequently been "debunked" by the CJEU as it has tended to favor the safeguarding of fundamental rights in its data protection jurisprudence.[57]

2.2 National Security in Data Protection Jurisprudence

National security is the sole responsibility of each Member State which follows from Article 4(2) TEU. The protection of national security serves indirectly the need to protect the rights and freedoms of others such as the

[50] See Article 1 Data Retention Directive.

[51] Digital Rights Ireland and Others (not 48), para 71.

[52] Judgement of 6 October 2015, Schrems, C-362/14, EU:C:2015:650 (Schrems I), para 94–95.

[53] Schrems I (not 52), para 106.

[54] Opinion 1/15 Accord PNR EU-Canada, EU:C:2017:592 (Opinion 1/15), para 232.

[55] Judgement of 16 July 2020, Facebook Ireland and Schrems, C-311/18, EU:C:2020:559 (Schrems II), para 199–201.

[56] Groussot, X., & Atik, J. (2021). A Weaponized Court of Justice in Schrems II. *Nordic Journal of European Law*, 4(2), 1–21, 3.

[57] Yeung, K. (1), & Bygrave, L. A. (2). (2022). Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. *Regulation and Governance*, 16(1), 150.

right to life recognized in Article 2 of the Charter and the right to liberty and security recognized in Article 6 of the Charter.

As implied by the title of this thesis, *Ligue des droits humains* concerns the conflicting interests of data protection and national security, a topic that has mostly been made relevant in relation traffic and location data in the jurisprudence of the Court.[58] *Ligue des droits humains* concerns the processing of PNR data, not traffic and location data. The case law of the Court is however highly relevant since the purposes for which personal data is processed are the same.

In *Digital rights Ireland* the CJEU recognized national security, specifically combatting international terrorism and serious crime threatening public security, as capable of justifying interferences with the right to data protection.[59] Further developing its case law, in *Privacy International* and *La Quadrature du Net* the CJEU declared that the prevention and punishment of activities that could threaten society, the population, or the State itself, such as terrorist activities, are of *particular significance*, taking into consideration the Member States' sole responsibility of its own national security.[60] Safeguarding *national* security thus goes beyond and can justify more serious interferences with the fundamental rights than the broader objectives of combating crime in general, even serious crime, and of safeguarding *public* security.[61] In *Commissioner of An Garda Síochána* the CJEU upheld the strict differentiation in degree of importance between the objectives and declared that even particularly serious crime cannot be treated in the same way as threats to national security.[62]

2.3 Case C-817/19 *Ligue des droits humains*

[58] Digital Rights Ireland and Others (not 48); Judgement of 21 December 2016, Tele2 Sverige and Others, C-203/15 and C-698/15, EU:C:2016:970; Judgement of 6 October 2020, Privacy International, C-623/17, EU:C:2020:790; Judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791; Judgement of 5 April 2022, Commissioner of An Garda Síochána, C-140/20, EU:C:2022:258. With the exception of *Opinion 1/15* (not 54) which concerns PNR data. Furthermore, see recent cases that were delivered after *Ligue des droits humains* and will not be discussed further in this thesis, Judgement of 20 September 2022, SpaceNet, C-793/19 and C-794/19, EU:C:2022:702; Judgement of 20 September 2022, VD and SR, C-339/20 and C-397/20, EU:C:2022:703.

[59] Digital Rights Ireland and Others (not 48), para 42.

[60] Privacy International (not 58), para 74; La Quadrature du Net and Others (not 58), para 135.

[61] Privacy International (not 58), para 75; La Quadrature du Net and Others (not 58), para 136.

[62] Commissioner of An Garda Síochána (not 58), para 61–63.

The Belgian Constitutional Court referred ten questions to the CJEU as it was faced with a case brought in front of it by a Belgian human rights organization, Ligue des droits humains (the human rights league). The questions referred concerned, among other things, the validity of the Passenger Name Record (PNR) Directive[63] in relation to its possible interference with the rights guaranteed in Articles 7, 8, and 52(1) of the Charter.

The PNR Directive sets up a system under which information (PNR data) about persons travelling by air to, from, or in some cases within, the EU can be accessed by national authorities for the purposes of combatting terrorist offences and serious crime. The objectives of the directive are, on the one hand, to ensure security and protect the life and safety of persons, and, on the other hand, to create a legal framework for the protection of PNR data with regard to their processing by competent authorities.[64] Processing operations include the transfer, collection, retention, assessment, matching against databases, disclosure, and erasure of PNR data.[65] The authority responsible for such processing operations is the "passenger information unit" (PIU) which is established by each Member State.[66] The PIU is responsible for retaining the collected PNR data for five years.[67] After six months, stricter rules for the disclosure of data apply and the data shall be anonymized by masking out personal identifications.[68]

Ligue des droits humains had pleaded that Belgian law which transposed EU law[69] into national legislation should be fully or in part annulled because of its interference with the rights to respect for private life and the protection of personal data, as well as the freedom of movement. The law was contested for being too wide in its scope and definition. The definitions of 'data' and 'passenger' were argued to be too broad, allowing for collection of data that indirectly would reveal sensitive information about the persons concerned and leading to the systemized and indiscriminate automated processing of such data of all passengers. The rules for automated processing and data-

[63] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJ L 119/132.

[64] Recital 5 PNR Directive.

[65] Article 6 PNR Directive.

[66] Article 4 PNR Directive.

[67] Article 12(1) PNR Directive.

[68] Article 12(2) & 12(3) PNR Directive.

[69] **The PNR Directive**, the **API Directive** (Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data), and in part **Directive 2010/65/EU** of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC Text with EEA relevance.

matching were argued to be insufficiently clear and the five-year period under which data retention is allowed disproportionately long.[70]

In dispute of those arguments, the Council of Ministers claimed that the national law in question was both proportionate in its aim and necessary to combat terrorism and serious crime.[71]

Through its examination, the Court upheld 'a general principle of interpretation' meaning it must avoid, as far as possible, interpretations that would affect the validity of an EU act.[72] Reading the PNR Directive in light of the Charter, the Court found that the provision "lent themselves" to interpretations that were consistent with primary law.[73] Some of the Court's interpretations did, however, confine the directive in comparison to how it had been interpreted by the Belgian legislature and implemented into national law which will be further examined in Chapter 5. In conclusion, the CJEU declared that PNR Directive could be interpreted in a way that ensures its conformity with the Charter and that its examination had revealed nothing capable of affecting the directive's validity.[74]

[70] Ligue des droits humains (not 17), para 51–55.
[71] Ligue des droits humains (not 17), para 56.
[72] Ligue des droits humains (not 17), para 86. See Chapter 5.1 below.
[73] See i.e. Ligue des droits humains (not 17), para 213 & 227.
[74] Ligue des droits humains (not 17), para 228.

3 What is Data Protection?

When the Charter was established in 2000 it provided novelty in including a right to protection of personal data as enshrined in its Article 8, partly deriving from the constitutionalizing of secondary EU data protection law, the ECHR, and Convention 108.[75] Although established in 2000, the Charter did not enter into force until the adaptation of the Lisbon Treaty[76] in 2009. The rights enshrined in Articles 7 and 8 of the Charter were however influential already before that through praxis of the CJEU.[77] In this Chapter I aim to explain what data protection entails on a constitutional level in the EU legal system.

3.1 The Charter Right to Protection of Personal Data

Data protection as enshrined in the Charter has a fundamentally different aim than data protection in secondary law. Drawing on the theories of Dworkin, Yeung and Bygrave argue that fundamental rights primarily protect moral values.[78] Consequently, fundamental rights are aimed at safeguarding "*moral values* associated with the inherent dignity of persons, rather than concerned primarily with safeguarding individuals against tangible harms".[79] Correspondingly, the Charter right to data protection is, unlike the provisions in secondary law, not necessarily aimed at protecting an individual in a given specific situation, but to preserve human dignity and protect the boundary between right and wrong, not "legally", but morally. Secondary data protection law, or "the European data protection regime" however upholds the values enshrined in the Charter and the regime as a system is a precondition to the realization of the fundamental rights.[80]

Article 8 of the Charter guarantees *the fundamental right to protection of personal data* which is a qualified right meaning limitations to it are tolerated. Limitations follow from Article 52 of the Charter, but unlike most other Charter tights, limitations are also provided directly in Article 8. These limiting conditions are (1) fair processing (2) purpose limitation (3a) based on consent, or (3b) another legitimate basis (4) provided for by law (5)

[75] González Fuster, G., & Gutwirth, S. (2013). Opening up personal data protection: A conceptual controversy. *Computer Law & Security Review*, 29(5), 531–539, 535.

[76] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, OJ C 306, 17.12.2007; entry into force on 1 December 2009.

[77] Judgement of 29 January 2008, Promusicae, C-275/06, EU:C:2008:54, para 63-64.

[78] Yeung & Bygrave (not 57), 143.

[79] Yeung & Bygrave (not 57), 143.

[80] Yeung & Bygrave (not 57), 144.

providing individuals the right to access and rectification of their data, and (6) imposing an independent supervisory authority.[81]

Data protection legislation mainly revolves around four types of actors. The individual, commercial actors, state actors such as public authorities or law enforcement agencies, and independent supervisory authorities.[82] These all have separate interests that are balanced by data protection legislation. The power asymmetry between the data subject and the actors who want to collect and process their data can "compound a feeling of hopelessness on the part of individuals".[83] Data protection legislation aims, by extension, to counteract this inherent power imbalance and preserve the autonomy of the individual.

The data subject's control is however not absolute and reliance on it alone does not provide an effective protection of the right to data protection.[84] Lindroos-Hovinheimo argues that the data subject is constructed as an autonomous subject with the illusion of control and the freedom of choice, mainly manifested through the data subject's ability to consent to data processing and access to claimable judicial remedies.[85] These elements are reflected in Article 8(2) of the Charter. Other aspects of data protection construct a passive subject that is not in control of their personal data,[86] which is reflected in the alternative of a legitimate basis to the individual's consent for processing.[87] Such more 'paternalistic' aspects of data protection consist of the instituting of an independent supervisory authority to oversee the relationship between the other actors and the requirement of fair processing, purpose limitation, and legal basis laid down in Articles 8(2) and (3).

In *Ligue des droits humains* the ground for processing of personal data is the legitimate basis of combatting terrorism and serious crime,[88] thus making the consent of the individual irrelevant and rather engaging the construction of a passive individual. Many of the exemptions to personal data protection are motivated by objectives of law enforcement as most clearly exemplified by

[81] Articles 8(2) & (3) the Charter.

[82] By comparison see Greenstein (not 5), 52.

[83] Lynskey (not 11), 12.

[84] Lynskey (not 11), 257.

[85] Lindroos-Hovinheimo, S. (2022) Individualism eller sammanflätade liv? En undersökning av integritetsskyddets filosofiska grundvalar, *Europarättslig tidskrift*, 25(1), 60.

[86] Lindroos-Hovinheimo (not 85), 69.

[87] Article 8(2) the Charter.

[88] Article 1(2) PNR Directive.

the simultaneous adaptation of the General Data Protection Regulation (GDPR)[89] and Law Enforcement Directive (LED)[90] which has precedence.[91]

3.2 Prohibition or Legitimization of Personal Data Processing

Legal scholars have debated whether data protection as a main rule *prohibits* data processing or *permits* data processing, but only under certain limiting conditions.[92] The prohibitive approach regards Article 8(1) of the Charter; "[e]veryone has the right to the protection of personal data concerning him or her" as principal and imposing a prohibition, to which follows exemptions from article 8(2), (3), and 52(1) of the Charter. This division echoes the structure of Article 8(1) and 8(2) ECHR, to which EU data protection law historically has been associated.[93]

The permissive or legitimizing approach by contrast regards Article 8 wholly as a system that allows the processing of personal data and does not make a hierarchized division between the prohibition in 8(1) and the exemptions in 8(2) and (3). Article 8(1) is therefore seen as a general right,[94] while the conditions in Article 8(2) and (3) are regarded as features of the right itself, rather than limitations to the right, which accordingly follow from Article 52(1) only.[95] Conceptually the distinction is noteworthy although the conditions under 8(2), (3) and 52(1) need to be considered regardless of the order in which so is done and if done together or separately. In practice the distinguishment is arguably of marginal relevance.[96]

The CJEU has tended to demonstrate a prohibitive approach, as exemplified by cases *Digital Rights Ireland* and *Opinion 1/15*.[97] In *Ligue des droits humains* the Court clearly takes on a prohibitive approach, drawing on its previous case law. In determining the interference of the PNR Directive with

[89] 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 [2016] OJ L119/1.

[90] 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 [2016] OJ L119/89.

[91] See Article 2(2) GDPR.

[92] I.e. Lynskey (not 45), 359; González Fuster & Gutwirth (not 75), 531.

[93] González Fuster & Gutwirth (not 75), 532-533. Article 1(1) of the 1995 Data Protection Directive referenced the ECHR Article 8 and the CJEU has been influenced by the jurisprudence of the ECtHR.

[94] Lynskey (not 45), 360.

[95] González Fuster & Gutwirth (not 75), 533.

[96] Lynskey (not 45), 361; González Fuster & Gutwirth (not 75), 533.

[97] Lynskey (not 45), 360-361.

the Charter, the Court referenced Articles 7 and 8(1), notably not Article 8 as a whole.[98] Article 8(2) was referenced together with article 52(1) under the considerations of the justification for the interferences resulting from the PNR Directive.[99]

The Court stated that "the communication of personal data to a third party… whatever the subsequent use of the information communicated" and the retention of and access to personal data by public authorities regardless of if the information is sensitive or "the persons concerned have been inconvenienced in any way" interferes with the rights in Articles 7 and 8 of the Charter.[100] Although judging the interference with Articles 7 and 8 combined, this supports the claim that the Court has continued to take on a prohibitive approach regarding the right to data protection since the mere communication and retention of data as such constituted an interference with the Charter. Although the prohibitive approach may strengthen the right to data protection, its assumption that any processing of personal data, by default, is not allowed makes it hard "to square with existing societal practices and norms" and with the EU interest of promoting the free flow of personal data on the internal market.[101]

3.3 Data Protection & Proportionality

The core principles of data protection in European law, as identified by legal scholar Bygrave, include fair and lawful processing, minimality, purpose limitation, data subject influence, data quality, data security, sensitivity – and proportionality.[102] Proportionality, he argues, has become a fundamental data protection principle in its own, mainly through development in case law.[103]

According to the understanding of Dalla Corte proportionality exists on three levels in relation to data protection, "with reference to the limitation of rights in the Charter, to the general principle of proportionality in the Treaties, and to proportionality at a secondary level".[104] Proportionality on the different levels varies in method and purpose but are entangled. The CJEU has withheld that secondary data protection law must be interpreted in light of primary data protection law.[105] The proportionality imposed by the Charter thus becomes reflected in secondary law through the interpretations of the

[98] Ligue des droits humains (not 17), para 92.
[99] Ligue des droits humains (not 17), para 113.
[100] Ligue des droits humains (not 17), para 96.
[101] Lynskey (not 45), 361.
[102] Bygrave, L. A. (2014). *Data privacy law : an international perspective*. Oxford University Press, Chapter 5.
[103] Bygrave (not 102), 147.
[104] Dalla Corte (not 28), 3.
[105] Dalla Corte (not 28), 9.

CJEU, to the extent where proportionality has become a basic principle of data protection.

By means of article 5(4) TEU, data protection law is subject to proportionality and subsidiarity since it is an area of shared competence. In practice, however, the EUs extensive legislature leaves little to no room for nation measures and the Union thus in practice appears to have exclusive competence.[106] Data protection legislation has historically been permeated by proportionality in various forms which is significant since the CJEU has expressed that legislation needs to be considered in its historical context.[107] Another important factor is that data protection in the EU is a hybrid instrument that serves the dual purposes of protecting fundamental rights alongside economic objectives.[108] The friction between these, often conflicting, purposes is at the very core of EU data protection. One of its main functions is therefore to balance multiple interests.

3.4 Data Protection & Privacy

Lynskey claims that while data protection and privacy heavily overlap, they are best understood as separate, partly because the functions of data protection are still a process in the making.[109] *The right to respect for private and family life* enshrined in Article 7 or the Charter protects the right to privacy.[110] Already before the Charter entered into force, the CJEU stated that individuals have a right to correct and lawful processing, access, and ratification of personal data by means of the right to privacy.[111] Even after the adaptation of the Charter the Court has derived a right of access to personal data from the right to privacy, confirming that some aspects of data protection are enshrined in article 7 of the Charter independently.[112]

Since the Charter was adopted, the CJEU has tended to refer to privacy and data protection rights, or Articles 7 and 8 of the Charter, together in its judgments.[113] The Court has also tended to suggest that data protection rights are conferred in Article 7 implicitly, while they are explicit in Article 8. In *Digital Rights Ireland* the CJEU stated that "the explicit obligation" in Article 8 is especially important for the rights guaranteed by Article 7.[114] In *Canada PNR* a similar claim was made that Article 8(1) "expressly confers" a right to

[106] Dalla Corte (not 28), 6.
[107] Dalla Corte (not 28), 6.
[108] Lynskey (not 11), 132.
[109] Lynskey (not 11), 105.
[110] Lynskey (not 11), 89.
[111] Judgement of 7 May 2009, Rijkeboer, C-553/07, EU:C:2009:293.
[112] Opinion 1/15 (not 54), para 219.
[113] I.e. Volker & Eifret (not 47), para 47; Schrems II (not 55), para 169–170; Privacy International (not 58), para 53; Ligue des droits humains (not 17), para 92 & 111–112.
[114] Digital Rights Ireland and Others (not 48), para 53.

data protection, unlike Article 7.[115] This line of argumentation is in line with the interpretations by the ECtHR regarding Article 8 of the ECHR.[116] There is an underlying presumption that protection of personal data leads to protection of private life and privacy.[117] Privacy is at the core of data protection, and vice versa.

Data protection and privacy rights are evidently related and often referenced and understood as an entity. Following this logic, the right to data protection is sometimes considered a narrower right that is included in privacy, or a mere vehicle to achieve privacy rather than a means in itself. Legal scholar Lynskey claims that such understandings of data protection are unsatisfactory because they do not recognize that data protection serves additional purposes than those of privacy.[118] She even concludes that data protection rights offer a broader protection than those of privacy.[119] Similarly, Bygrave argues that although privacy is central to it, data protection relates to a vast array of interests such as personal autonomy, integrity, dignity, pluralism, and democracy.[120]

Another way to differentiate data protection from privacy is through a permissive approach to the right to data protection. Privacy is clearly prohibitive in nature while data protection offers ambiguity in this sense.[121] While privacy aims to protect the private sphere that is private and family life, data protection does not necessarily aim to keep data private, meaning undisclosed, anonymous, or secluded. For example, a person (data subject) about whom there is information (personal data) is not necessarily in possession of the data regarding them. Often data is controlled by another party, such as a bank, employer, company, or health care provider etc. Keeping data private would thus mean that the data subject does not have access to the data they are subject to. Contrary to common belief the fundamental right to protection of personal data as enshrined in article 8 of the Charter in its early appearances originated from the right to access to information rather than privacy.[122]

Often it is both necessary and desirable to share personal data for the functioning of society. If data processing per se is not prohibited, but *unlawful* processing is, data protection acts as a tool of transparency, in differentiation to privacy which is a tool of opacity.[123] Having their conceptual differences,

[115] Opinion 1/15 (not 54), para 133.
[116] Amann v. Schweiz; Rotaru v. Rumania (not 42).
[117] Lindroos-Hovinheimo (not 85), 60.
[118] Lynskey (not 11), 102.
[119] Lynskey (not 11), 129.
[120] Bygrave, L. A. (2002). *Data protection law : approaching its rationale, logic and limits*. Kluwer, 134–136.
[121] González Fuster & Gutwirth (not 75), 536.
[122] González Fuster & Gutwirth (not 75), 535.
[123] González Fuster & Gutwirth (not 75), 536.

data protection is necessary to ensure the right to privacy and the right to protection of personal data is enshrined directly in Article 7 of the Charter. Further, the enforcement of Article 8 is essential to protect the rights guaranteed in Article 7 of the Charter. This is particularity evident in the case law of CJEU since the rights are often referred together and interference with the rights is not always distinguished.

3.5 Privacy, Surveillance, & Human Dignity

Technological development is commonly associated with progress, improvement, and innovation. This is evident for example in the EU strategy for a Europe fit for the digital age. While the risks that arise from technological development are highlighted in the strategy, it focuses on the benefits of digital solutions and how they can "enrich the lives of all of us".[124] As noted in the introduction to this thesis, technology also offers potential downsides, such as the manipulation of human behavior by the use of predictive modelling.[125] Technology can also indirectly threaten democracy by more emotional aspects such as 'the feeling of surveillance'.

> There is a certain discomfort associated with being constantly monitored. There is also the feeling of helplessness in being characterised or depicted in a manner that does not correspond with a self-image. Being categorized in a certain light, based on data points, statistics, mathematics, machine learning and artificial intelligence, where human action is predicted based on probability, is harmful to humans. Adding insult to injury, there is no means of altering this image as it is created by the 'black box' of technology and the logic of which is accessible to only a few.[126]

The quote above demonstrates how surveillance and profiling, or even the idea of these hidden concepts affects to the human psyche. Fictional dystopias of government surveillance such as Orwell's Nineteen Eighty Four have interestingly played a role in the promoting the distinctive fundamental rights character of European data protection law.[127] In light of the expansion of data usage, and with it the expansion of data itself, the potential for unwanted forms of surveillance is expanding with it.

[124] European Commission, "Communication from the Commission to the Euro-pean Parliament, the Council, the European Economic and Social Committee of the Regions, *Shaping Europe's digital future*" COM (2020) 67 final, 1.

[125] Greenstein (not 5), 431; Zuboff (not 7), 100.

[126] Greenstein (not 5), 146.

[127] Yeung & Bygrave (not 57), 144.

In *Digital Rights Ireland* the Court stated that certain forms of data retention might generate "in the minds of persons concerned the feeling that their private lives are the subject of constant surveillance".[128] Particularly that the data subjects were not informed of the data use and retention was pointed out as relevant in generating the feeling.[129] Such a feeling has the potential to have an inhibiting effect on the way people act and interfere with fundamental rights and thus poses a threat to human dignity. Data protection and privacy can be understood as tools aimed at ensuring human dignity, of which the right to personality and self-development are important aspects.[130]

This notion has been further deliberated in the ECtHR case *Big brother Watch and Others v. UK (No. 2)* by the concurring opinion of Judges Lemmens, Vehabović and Bošnjak.[131] The Judges held that the mere feeling of constant observation can have serious effects on one's mental and physical well-being and that such surveillance exerts both internal and external pressures on freedom, making people less likely to exercise their civil rights.[132] The Judges' concurring opinion aimed to emphasize the importance of privacy protected by Article 8 ECHR in relation to interference in the form of mass surveillance, a point the Judges felt was not upheld enough in the judgement. They argued that "privacy is a fundamental precondition for a variety of fundamental individual interests, but also for the existence of a democratic society".[133]

In *Ligue des droits humains* the Court concluded that the PNR directive entailed serious interferences with Articles 7 and 8 of the Charter since the system set up by the PNR Directive "seeks to introduce a surveillance regime that is continuous, untargeted and systematic, including the automated assessment of the personal data of everyone using air transport services".[134] In his opinion on *Ligue des droits humains*, Advocate General Pitruzzella pointed out particularity the large amounts of available data, the usage of technology to link and combine data, and the increasingly common use of such technology, specifically for the purposes of preventing certain forms of serious crime, as cumulatively amplifying the seriousness and risking to favor "a gradual slide towards a 'surveillance society'".[135]

[128] Digital Rights Ireland and Others (not 48), para 37.

[129] Digital Rights Ireland and Others (not 48), para 37.

[130] Lynskey (not 11), 95.

[131] Joint partly concurring opinion of Judges Lemmens, Vehabović and Bošnjak, in Big Brother Watch and Others v. the United Kingdom (No. 2) [GC], App nos 58170/13, 62322/14 and 24960/15, 25 May 2021.

[132] Joint partly concurring opinion in Big Brother Watch v. UK (not 132), para 4–8.

[133] Joint partly concurring opinion in Big Brother Watch v. UK (not 132), para 1 & 3.

[134] Ligue des droits humains (not 17), para 111.

[135] Opinion of Advocate General Pitruzzella delivered on 27 January 2022, Ligue des droits humains, C-817/19, EU:C:2022:65, para 80.

4 Limitations on Data Protection

As important as data protection may be, the right to protection of personal data is not an absolute right, nor is the right to privacy.[136] Certain infringements are accordingly tolerated. Some limitations to the right are found directly in Article 8 and have been accounted for above. Article 51 of the Charter limits its scope and Article 52 of the Charter lays down the conditions under which the exercise of a right recognized by it can be limited.

Limitations must be provided for by law and respect the essence of those rights. Limitations must also be proportional, necessary, and genuinely meet objectives of general interest or the need to protect the rights and freedoms of others.[137] As has been mentioned, the rights provided for by the Charter also need to at least correspond with the rights provided for by the ECHR.[138] The scope of the Charter is limited by the scope of EU law.[139]

4.1 Provided for by Law

As a first condition, any limitation to a right must be provided for by law which follows from Article 52(1) the Charter and has been elaborated on by the CJEU in its interpretations. The requirement for a legal basis can also be found directly in Article 8(2).

It is the settled case law of the Court that the scope of a limitation must be provided for by the law that the limitations is based on.[140] Any legislation that constitutes an interference with the fundamental rights provided for by the Charter can thus on the one hand be considered a legal basis for doing so – justifying the interference, or on the other hand, if it is insufficient in providing clear and precise enough measures, be invalidated for being incompatible with the Charter. The Court has further developed the requirement, dividing the assessment of the legal basis into two factors, the 'formality' of the law and the 'quality' of the law.

In line with the wording of Article 52(1) of the Charter, the 'formal requirement' entails that the *law* is an instrument that is legally binding under domestic law.[141] The 'quality requirement' concerns the purpose of the provision, thus using a teleological method of interpretation. As elaborated

[136] Compare i.e. Recital 4 GDPR.
[137] Article 52(1) the Charter.
[138] Article 52(2) the Charter. See also Chapter 1.3.2 above.
[139] Article 51 the Charter.
[140] Opinion 1/15 (not 54), para 139; Schrems II (not 55), para 175; Privacy International (not 58), para 65.
[141] La Quadrature du Net and Others (not 58), para 132.

on by Advocate General Pitruzzella in his opinion, the criterion "is not only intended to secure compliance with the principle of lawfulness… but reflects a need for legal certainty".[142] Legal certainty demands that the limits of the interference, if found legitimate, are not exceeded thus relating to the proportionality of the interference. By the wording of Article 52(1) of the Charter the 'provided for by law' criterion is not explicitly subject to the principle of proportionality. In praxis, however, the method that has been established by the CJEU for assessing of the 'quality' of the law is as a part of the proportionality analysis.[143]

In *Digital Rights Ireland* the Data Retention Directive was found insufficient in limiting the extent of the interference with the rights provided for by the Charter.[144] The directive did not ensure that the interference would be limited to what was strictly necessary which led to the CJEU concluding to declare the directive void.[145] Further, the CJEU has stated that to ensure that a measure is limited to what is strictly necessary, the legislation must "lay down clear and precise rules governing the scope and application […] and imposing minimum safeguards" as well as "indicate in what circumstances and under which conditions" a measure may be adopted.[146] The need for such minimum safeguards is greater when sensitive data is processed or when automated processing is carried out.[147] The law must also provide objective criteria that establish a link between the processing of data and the purposes the law pursuits.[148]

In other words, the scope and application must be clear and provided for directly by the law, the circumstances and conditions, however, need only be *indicated* as long as there is an objective link, leaving room for the proportionality principle to be given due regard. The concept of proportionality, and especially necessity, is therefore relevant in relation to the provided for by law criterion.

Deriving from its previous case law, in *Ligue ds droits humains* the Court assessed the 'quality' of the law as part of the proportionality analysis stating that the "question is largely the same as that of compliance with the proportionality requirement".[149] While declaring that the scope and limitation of the interference must be provided for directly by the law, the Court also held that

[142] Opinion of Advocate General Pitruzzella (not 135), para 85.
[143] I.e. Schrems II (not 55), para 180; La Quadrature du Net and Others (not 58), para 132.
[144] Digital Rights Ireland and Others (not 48), para 65.
[145] Digital Rights Ireland and Others (not 48), para 69.
[146] Tele2 Sverige and Others (not 58), para 109.
[147] Opinion 1/15 (not 54), para 141.
[148] La Quadrature du Net and Others (not 58), para 133.
[149] Ligue des droits humains (not 17), para 119.

> that requirement does not preclude the limitation in question from being formulated in terms which are sufficiently open to be able to adapt to different scenarios and keep pace with changing circumstances [and that]… the Court may, where appropriate, specify, by means of interpretation, the actual scope of the limitation in the light of the very wording of the EU legislation in question as well as its general scheme and the objectives it pursues, as interpreted in view of the fundamental rights guaranteed by the Charter.[150]

In doing so, the Court has seemingly given itself a wide margin of interpretation of the provided for by law requirement and the 'quality' of the law. As will be demonstrated below, some interpretations of the PNR Directive rely heavily on reading its provisions in light of the Charter and in accordance with the clarifications made in the judgement by the Court.

4.2 Respecting the Essence

Any infringement of a right provided for by the Charter must respect its essence.[151] It is thus relevant to look at what the essence of the right to data protection entails and what respect for such a right means. The CJEU uses the term 'not adversely affect' as alternative to 'respect' meaning that the essence of a fundamental right is respected if it is not adversely affected.[152] The concept of essence has attracted the attention and engagement of legal scholars debating what the added value of the test consists of, which will be demonstrated below.

4.2.1 The Concept of Essence

Qualified rights are not absolute and can thus be infringed – a truth with modification according to the opinion of some legal scholars. The President of the CJEU, Koen Lenaerts, has written an article on the topic in which he stresses that the essence of fundamental rights, or "our core values as Europeans" are absolute and cannot be subject to balancing.[153] The CJEU should therefore never carry out a proportionality analysis after interference with the essence of a right has been established.[154]

A similar approach has been advocated by Brkan, arguing that the concept of essence functions to accentuate "the inalienable nature of fundamental rights"

[150] Ligue des droits humains (not 17), para 114.
[151] Article 52(1) the Charter.
[152] See examples below.
[153] Lenaerts, K. (2019). Limits on Limitations: The Essence of Fundamental Rights in the EU. *German Law Journal*, 20(6), 782.
[154] Lenaerts (not 153), 788.

but also offers additional protection of the Charter rights.[155] While proportionality draws a line between proportionate and disproportionate interferences, essence draws a line between disproportionate interferences and interferences that could never be proportionate. Respect for the essence of a right is therefore a precondition to proportionality.[156] This methodology, Brkan states, has regrettably not been fully embraced by the CJEU since occasionally the essence is weight into the proportionality assessment.[157]

In their understanding of the concept of essence, Lenaerts and Brkan proclaim an 'absolute theory'. There are also more 'relative theories', according to which there is not necessarily an absolute essence of a right excluding the measure from being subject to proportionality. According to such conceptions interference with the essence rather indicates that the proportionality analysis needs to be done more strictly.[158]

Hallinan points out the difficulty in finding a definition of essence that has a unique function in relation to the concept of proportionality.[159] Since the concepts are troublesomely separated, the "utility and clarity of any description will rise according to the degree to which it can specify the relationship between the two concepts".[160] Advocating a relative approach, he finds the concept of essence in relation to Article 8, as it has emerged in the jurisprudence of the Court so far, to be best described as "a normative pivot".[161] This definition of essence is auxiliary to proportionality, its function to distinguish certain disproportionate infringements as extra egregious, and a defining trait that its concept and boundaries remain open and flexible until the CJEU provides further guidance.[162]

Other potential approaches claim that the concept of essence serves to avoid that the right is completely eliminated or completely disregarded, thus ensuring that the right is not abolished and that at least some "meaningful efforts to limit the range and nature of their infringements" are made.[163] This approach was arguably demonstrated by the CJEU in *Schrems I* in relation to Article 47 of the Charter as the right to a judicial remedy had been abolished.[164] Drawing from analogy to international law, the concept of

[155] Brkan, M. (2019). The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning. *German Law Journal*, 20(6), 864–883, 869.

[156] Brkan (not 155), 868, 883; Dalla Corte (not 28), 16.

[157] Brkan (not 155), 875.

[158] Dawson, M., Lynskey, O., & Muir, E. (2019). What Is the Added Value of the Concept of the Essence of EU Fundamental Rights. *German Law Journal*, 20(6), 767.

[159] Hallinan, D. (2021). The Essence of Data Protection: Essence as a Normative Pivot. *European Journal of Law & Technology*, 12(3), 62– 63.

[160] Hallinan (not 159), 63.

[161] Hallinan (not 159), 70.

[162] Hallinan (not 159), 79.

[163] Dawson, Lynskey, & Muir (not 158), 767.

[164] Schrems I (not 52), para 94–95.

essence may also serve as a minimum guarantee for rights that requires the action of the state, thus indicating what the minimum level is that the state needs to entertain regardless of external factors.[165] Dalla Corte argues that the added value of the essence test is at best very limited and at worst could lead to an increase in arbitrariness of the Court's limitations analysis.[166] Since the essence test is value-based it offers an opt-out for the Court to compensate for its over-reliance on the threshold requirements of the proportionality test.[167]

In his opinion on *Ligue des droits humains*, the Advocate General demonstrated a clearly absolute approach to the concept of essence stating that "any fundamental right represents a 'hard nucleus' that guarantees to each and every individual a sphere of liberty that must always remain free from interference by the public authorities and may not be subject to limitations" and that essence is an autonomous test which "must be determined before and independently of evaluation of whether the measure complained of is proportionate".[168] In doing so the Advocate General acceded to the opinions of the President of the CJEU.[169] The CJEU did not comment in such dept on the methodology of the essence test but came to the same conclusion as Advocate General Pitruzzella regarding the contents of the essence. The Court only carried out a proportionality analysis after establishing that the essence of the fundamental rights had not been adversely affected and thus followed the methodology proposed by Lenaerts in his article on the subject.[170]

4.2.2 The Contents of the Essence of Data Protection

Since the right to data protection is a relatively young right, its essence is still being shaped. What can be concluded so far from the case law of the CJEU regarding the contents of the essence of the right to data protection follows below.

Of relevance to the essence of the rights laid down in Article 7 of the Charter is the nature of the data in question and what it reveals about the person it concerns. In relation to the processing of personal data collected from the use of electronic communication devices, the CJEU has established that the *contents* of the communications cannot be revealed without adversely

[165] Dawson, Lynskey, & Muir (not 158), 767–768.

[166] Dalla Corte (not 28), 17.

[167] Dalla Corte (not 28), 16.

[168] Opinion of Advocate General Pitruzzella (not 135), para 91. Interestingly the Advocate General referenced *Schrems I* in his defence of the absolute theory, a case which by scholars has been understood as not fully aligned with an absolute approach (See Brkan (not 155), 875).

[169] Lenaerts' article (not 153) is directly cited in note 83 of the opinion.

[170] See Chapter 5.2.1 below.

affecting the essence.[171] In other words, data about for example telephone traffic, location, phone numbers, calls, and messages (traffic and location data) may be revealed, but not the contents of those calls or messages. The Court has in another case argued that even when the content of communications is not revealed, such data which enables the setting up of a profile is "no less sensitive, having regard to the right to privacy, than the actual content of communications" since it can allow for very precise conclusions to be drawn concerning an individual's private life.[172] However, the Court did not consider the use of such other data capable of adversely affecting the essence of the right.[173] In relation to PNR data about air passengers traveling between Canada and the EU (PNR data), the CJEU considered the information to be limited enough to that specific context and thus only revealing certain aspects of private life which did not adversely affect the essence of the right to private life.[174]

The essence of Article 8 is dependent on its understanding as either prohibitive or permissive, or if the essence of the right is enshrined in Article 8(1) only or Article 8 as a whole.[175] Under the prohibitive approach, the essence of data protection is prohibition of all processing of personal data. The permissive approach regards the essence as multiple requirements and thus as an already limited right which by default allows for certain interferences.[176]

The CJEU has stated that the essence of the rights laid down in Article 8 of the Charter was not adversely affected when "the principles of data protection and data security" were respected, especially that proper technical and organizational measures were in place, protecting the data from accidental or unlawful loss or alteration.[177] The provision in question also laid down rules ensuring that only authorized personnel could access the data and that the data should be destructed at the end of the retention period.[178] These aspects were not explicitly pointed out by the Court as relevant, but since the provision was referred, perhaps implicitly relevant. In another case the Court emphasized that the essence was respected because the purposes for processing were defined and that there were rules to ensure the security, confidentiality, and integrity of the data.[179]

In *Schrems I* the Court found that the act did not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47

[171] Digital Rights Ireland and Others (not 48), para 39; Schrems I (not 52), para 94.
[172] Tele2 Sverige and Others (not 58), para 99.
[173] Tele2 Sverige and Others (not 58), para 101.
[174] Opinion 1/15 (not 54), para 150–151.
[175] See Chapter 3.2 above.
[176] González Fuster & Gutwirth (not 75), 533.
[177] Digital Rights Ireland and Others (not 48), para 40.
[178] Digital Rights Ireland and Others (not 48), para 16.
[179] Opinion 1/15 (not 54), para 150–151.

of the Charter since individuals completely lacked access to judicial remedies for the purposes of access, rectification, or erasure of their personal data.[180] In the case the Court only comment on the essence of Articles 7 and 47, not Article 8 of the Charter.[181] Interestingly, the Court found that the measure interfered with the essence of the right to an effective judicial remedy, not the right to protection of personal data. From Article 8(2) of the Charter follows that everyone has the right of access to and rectification of personal data concerning them. The complete lack of judicial remedies could therefore have been understood as not respecting the essence of the rights enshrined in Article 8 of the Charter. Taking on a prohibitive approach to Article 8, its essence lies in Article 8(1) alone and not 8(2). Purpose limitation, however, is enshrined in Article 8(2) and was nonetheless considered to constitute the essence of data protection in *Opinion 1/15*. The logic of the prohibitive or premising approach seems therefore to have an ambiguous relationship to the essence of the right to data protection.

In conclusion, drawing on the jurisprudence of the CJEU, the essence of data protection seems to consist of data safety and purpose limitation. The right to an effective judicial remedy regarding access, rectification, and erasure of personal data that is enshrined in Article 8(2) of the Charter has been protected, but as part of the essence of the right to an effective remedy. The essence of the right to private life is related to the contents of the personal data and to what extent the data reveals sensitive information about a person's private life.

In *Ligue des droits humains* the CJEU declared that "the interferences which the PNR Directive entails do not adversely affect the essence of the fundamental rights enshrined in Articles 7 and 8 of the Charter".[182] The Court upheld its case law and confirmed its previous findings regarding the contents of the essence of privacy and data protection. Since PNR data is limited to the context of air travel and does not allow "a full overview of the private life of a person" the Court did not consider the essence (of privacy) affected.[183] Nor was the essence (of data protection) affected since the PNR Directive fulfilled the requirement of purpose limitation and laid down sufficient "rules governing the transfer, processing and retention… 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".[184]

4.3 Proportionality

[180] Schrems I (not 52), para 95. See Brkan (not 155), 868.

[181] Schrems I (not 52), para 94–95.

[182] Ligue des droits humains (not 17), para 120.

[183] Ligue des droits humains (not 17), para 120. Of relevance was also that the PNR Directive expressly prohibits processing of sensitive data.

[184] Ligue des droits humains (not 17), para 120.

Proportionality is a tool to balance interests.[185] It functions to provide legal certainty by minimizing the discretion of courts in their adjudications, however, proportionality reasoning inherently requires some degree of flexibility being left to the courts.[186] Leading to greater judicial scrutiny and accountability, the principle arguably has led to the strengthening of protection of human rights.[187] Proportionality is a fundamental EU principle that spans across the EU legal system. As demonstrated above, proportionality permeates data protection legislation in a multitude of ways. Proportionality is a requirement that needs to be met to legitimize the infringement of a Charter right. The requirement is confined in Article 52(1) of the Charter and reads as follows.

> 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.

4.3.1 The Sub-Tests of the Proportionality Analysis

Proportionality can be understood *lato sensu* (in general as an overall assessment) and *stricto sensu* (as the balancing or weighing of two competing interests).[188] In this thesis I refer to proportionality *lato sensu* unless specified otherwise. Deriving from the German constitutional tradition proportionality *lato sensu* entails suitability, necessity and *stricto sensu* proportionality. The proportionality analysis, as described by legal scholar Dalla Corte, consists of these three steps.[189] For a measure to be **suitable** it must be fit to achieve a goal that is recognized as worthy of pursuit by the judicial system. The **necessity** is met if the measure imposes the least interference with the right it restricts compared to other equally effective and suitable options. The third step, ***stricto sensu* proportionality**, is value based and aimed at ensuring that the goal pursued outweighs the interference with the right.[190]

Unlike Dalla Corte who identifies ‘proper purpose’ as part of the suitability sub-test, Stone Sweet and Mathews considers this step an independent step of the proportionality analysis, thus adding a first step of “legitimacy,” or “proper purpose”.[191] Their approach differentiates between the ends pursued

[185] Dalla Corte (not 28), 1.
[186] Dalla Corte (not 28), 17.
[187] Young, A. L. & Búrca, G.,” Proportionality.” in Vogenauer, S., & Weatherill, S. (2017). *General principles of law. European and comparative perspectives*. Hart Publishing, 133.
[188] Dalla Corte (not 28), 3.
[189] Dalla Corte (not 28), 3.
[190] Dalla Corte (not 28), 3–4.
[191] Stone Sweet & Mathews (not 30), 35.

by the interfering measure (as judged under step one, "proper purpose") and the suitability of that measure, or in other words that "a rational relationship exists between the *means chosen* and the *ends pursued*".[192] Regardless of the number of steps taken, the contents of the analysis are largely the same and each of the requirements must be met for a limitation to be considered proportional. The Court must also assess the importance of the proper purpose in order to verify that it is proportional to the seriousness of the interference.[193]

4.3.2 The Politics of Proportionality

To determine what is proportionate in the realm of data protection is not an easy task.[194] The first steps of the analysis (proper purpose, suitability, and necessity), or the 'means-end analysis' are threshold requirements meaning they result in a binary outcome of the requirement being met or not.[195] The last step, the *stricto sensu* proportionality sub-test, on the other hand, is a value-based act of balancing or in the words of Dalla Corte "a nuanced axiological assessment of the trade-off between the rights and freedoms involved" that does not result in a binary outcome.[196] The understanding of fundamental rights as a legal expression of moral values provides explanation as to why the balancing of rights, or the harm caused by interference with a right against its benefits, by nature is a moral, political, sensitive, and difficult task.[197] Accordingly, the balancing of fundamental rights, proportionality *stricto sensu*, is not a question of legal or illegal (a threshold requirement), but rather one of moral or immoral (a value-based judgement).

The CJEU has seemingly tended to favor safeguarding the fundamental right to protection of personal data, but the balance will shift depending on the "changing social, political, technical, economic and moral concerns and contexts".[198] Over the last years data protection legislation in the EU has expanded and consequently the interest has become more visible and recognized as increasingly important. Perhaps the current societal context has changed and shifted the circumstances in favor of national security. With a current war in Europe, the rise of right-wing nationalism, and a pandemic in the near past, national security interests may be gathering in on data protection interests.

In *Ligue des droits humains* the CJEU (and the EU legislature before it in adopting the PNR Directive) was faced with balancing the objectives of data protection and privacy against national security. To weigh the interest of

[192] Stone Sweet & Mathews (not 30), 36.
[193] La Quadrature du Net and Others (not 58), para 131.
[194] Dalla Corte (not 28), 2.
[195] Dalla Corte (not 28), 3.
[196] Dalla Corte (not 28), 12.
[197] See Chapter 3.1 above, with reference to Yeung & Bygrave (not 57), 143.
[198] Yeung & Bygrave (not 57), 150.

national security against data protection is indeed a task of political nature. As suggested by Dalla Corte, the Court seemingly tends to avoid *stricto sensu* proportionality balancing because it is value-based and therefore inherently of 'moral nature' and most often it is the necessity sub-test, or in some cases suitability sub-test, that fails in the Court's judgements.[199]

4.3.3 The 'Strictly Necessary Doctrine'

Since necessity is a sub-test to proportionality, the concepts of necessity and proportionality are heavily related. In its guidelines on proportionality, the European Data Protection Supervisor has stated that necessity is a precondition to proportionality.[200] Before the proportionality can be assessed, it should therefore first be clarified that the measure at hand is "the least intrusive effective measure available to attain the objective pursued".[201] Once it has been established that a measure is the least intrusive effective remedy available, the suitability, necessity and non-excessiveness of that measure can be considered through the proportionality analysis.

It is the settled case law of the CJEU, with reference to due regard to the principle of proportionality in Article 52(1) of the Charter, that derogations from and limitations on the protection of personal data should apply only in so far as is *strictly necessary*.[202] The 'strictly necessary doctrine' has led to the CJEU upholding a high threshold for the necessity sub-test of the proportionality analysis.[203] The more precise, targeted, and detailed, the more likely an interfering measure is to meet the requirement of strict necessity.[204] The lack of limitations regarding, for example, the length of the data retention period, the actors by whom data can be accessed and disclosed to, or the classification of data depending on its usefulness in relation to the objects pursued has led the Court to deem interfering measures not limited to what is strictly necessary.[205] The necessity sub-test has thus been given a narrow scope.

---

[199] Dalla Corte (not 28), 12.

[200] European Data Protection Supervisor, "*EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*" (25 February 2019) <https://edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf > accessed 22 October 2022.

[201] EDPS Guidelines (not 200), 12.

[202] Judgement of 7 November 2013, IPI, C-473/12, EU:C:2013:715., para 39; Digital Rights Ireland and Others (not 48), para 51–52; Schrems I (not 52), para 92; Opinion 1/15 (not 54), para 140; Tele2 Sverige and Others (not 58), para 96; Schrems II (not 55), para 176; La Quadrature du Net and Others (not 58), para 130; Commissioner of An Garda Síochána (not 58), para 52.

[203] Dalla Corte (not 28), 11.

[204] Dalla Corte (not 28), 12.

[205] See Digital Rights Ireland and Others (not 48), para 62–66.

5 Implications of *Ligue des Droits Humains*

In this Chapter I will examine how the CJEU reasoned in its judgement *Ligue des droits humains* in relation to the different aspects of data protection rights that I have presented above. In other words, how the fundamental right to protection of personal data affected the interpretation of the PNR Directive and by extension how the Charter, mainly Articles 7, 8, and 52(1), is enforced and affects secondary data protection legislation.

5.1 A General Principle of Interpretation

The Court has established a general principle of interpretation meaning that if it has the option to do so, the Court must avoid using its mandate to invalidate secondary law. Drawing on its previous case law, the Court stated that

> an EU act must be interpreted, as far as possible, in such a way as not to affect its validity and in conformity with primary law as a whole and, in particular, with the provisions of the Charter. Thus, if the wording of secondary EU legislation is open to more than one interpretation, preference should be given to the interpretation which renders the provision consistent with primary law rather than to the interpretation which leads to its being incompatible with primary law.[206]

The general principle of interpretation has been applied continuously by the Court in several cases dating back, at least to 1983.[207] To my knowledge, the principle has not previously been applied in a case concerning data protection. It has however been applied when reviewing the conformity of secondary law to the provisions of the Charter.[208] The question of the legislature's imposition of limitations on fundamental rights was relevant in two of the cases. In case

[206] Ligue des droits humains (not 17), para 86.

[207] Judgment of 13 December 1983, Commission v Council, C-218/82, ECR 4063, para 15.

[208] Judgement of 31 January 2013, McDonagh, C-12/11, EU:C:2013:43, para 44 (Articles 16, 17 & 52 of the Charter); Judgement of 19 September 2013, Review of Commission v Strack, C-579/12 RX-II, EU:C:2013:570, para 40 (Article 31(2) of the Charter); Judgment of 15 February 2016, N., C-601/15 PPU, EU:C:2016:84, para 48 (Article 6 & 52 of the Charter); Judgement of 14 May 2019, M and Others, C-391/16, C-77/17 and C-78/17, EU:C:2019:403, para 77 (Article 18 of the Charter); Judgment of 2 February 2021, Consob, C-481/19, EU:C:2021:84, para 50 (Articles 47 & 48 of the Charter).

N. concerning the Charter right to liberty and security vs. the interest of protecting of national security and public order,[209] and in *McDonagh* concerning the freedom to conduct a business and the right to property vs. the interest of upholding a high level of protection for consumers in the EU.[210] In both cases the Court abstained form declaring the act in question invalid.

The interpretation principle requires the Court to take into consideration primary law *as a whole* and, *in particular*, the provisions of the Charter. The right to data protection and privacy as enshrined in Articles 7 and 8 of the Charter need therefore to be considered together with other provision of primary law, in *Ligue des droits humains* most relevantly Article 4(2) TEU stating that national security is the sole responsibility of the Member States and Articles 2 and 6 of the Charter containing the rights to life, liberty, and security respectively.

5.2 Essence after Case C-817/19

The function of the concept of essence has not been settled and varies, according to scholars, from an absolute core or uninfringeable part of a right, to a flexible boundary serving to signal that a proportionality analysis needs to be done more strictly. The concept of essence has been made relevant, especially in relation to data protection. The first time the CJEU annulled legislation on the basis of interference with the essence of a right was in *Schrems I*.[211] This is perhaps illustrative of the unavoidability of interfering with the right to data protection or its permissive nature since processing of data is essential to the functioning of our society, which makes the concept of essence the more relevant.

5.2.1 An Absolute Approach to Essence

The Court found that the essence of the fundamental rights enshrined in Articles 7 and 8 of the Charter had not been adversely affected by the interferences of the PNR Directive, and the provisions thus 'passed' the essence test.[212] Although not adding any new guidance regarding the contents

[209] N. (not 208), para 50 ff. The case concerned the detention of an asylum applicant who had committed crime and illegally resided in the Member State of application, thus interfering with the right to liberty of the applicant in favour of the Member State's interest of national security. The Court concluded that the EU legislature had "struck a fair balance" between the interests (para 70).

[210] McDonagh (not 208), para 59–65. The case concerned the obligation of air carriers to provide care to passengers whose flight has been cancelled. The Court concluded that, in light of Article 38 of the Charter and Article 169 TFEU which both safeguard the interests of consumers, a fair balance of the competing interests had been struck (para 63–64).

[211] Schrems I (not 52), para 94–95.

[212] Ligue des droits humains (not 17), para 120.

of the essence of data protection,[213] the Court seemingly clarified its stance on the methodology and function of the essence test. The Court carried out an essence test *before* and *independently* of the proportionality analysis, thus acceding to the absolute approach as advocated by scholars such as Lenaerts and Brkan.[214] Even in choosing not to invalidate the PNR Directive, the CJEU upheld the concept of essence as providing a baseline of protection of the fundamental rights, and presumably, providing additional protection than that offered by the concept of proportionality.

5.2.2 A Relative Approach to Essence

Although the approach taken by the CJEU certainly indicates that the essence test will be carried out independently of proportionality, the relationship between the concepts of essence and proportionality still offers ambiguity and is not fully one of complete independence. Tendencies towards a more relative approach can also be distinguished in the case and the function of the concept of essence may therefore serve additional purposes.

In recent cases *Commissioner of An Garda Síochána*, *La Quadrature du Net*, and *Privacy International* that also concerned data protection (traffic and location data) in relation to national security, the concept of essence was not commented on in any detail by the Court or the Advocate General. Nor was the general principle of interpretation applied in those cases. In *Ligue des droits humains*, on the other hand, the concept of essence was judged upon. The relationship between the concept of essence and the general principle of interpretation is unclear but an interesting one. In the name of avoiding to invalidate the PNR Directive when multiple interpretations of it are available, the CJEU in a sense imposes on itself an obligation to limit the rights in Articles 7 and 8 of the Charter, perhaps to their essence thus making the concept more relevant.

Being one of the fundaments of data protection as enshrined in Article 8(2) of the Charter, the clear and conclusive definition of the purposes for which personal data may be processed is essential to guarantee its compliance. It is the settled case law of the CJEU that the principle of purpose limitation constitutes part of the essence of data protection, which makes its observation critical.[215] Since the PNR Directive lays down rules limiting these, the

[213] See Chapter 4.2.2 above. Of relevance the Court held that processing of sensitive data explicitly is prohibited, the nature of data is limited to air travel and does not allow for a full overview of the private life of a person, the directive lays down rules limiting the purpose for processing, and data security is observed.

[214] See Chapter 4.2.1 above.

[215] See Chapter 4.2.2 above.

essence was not adversely affected.[216] The mere existence of rules regulating the processing purposes was therefore enough to satisfy the essence test.

In its judgement, the Court continuously ensured that the principle of purpose limitation was upheld, also in relation to proportionality and necessity. The Court declared that data collected under the system set up by the PNR Directive could not be processed for other or additional purposes, clarifying that the directive needs to be interpreted in such a way that those purposes are exhaustive.[217] To ensure this the Court concluded that PNR data cannot be retained in a database that can also be consulted for other purposes and that national legislation allowing for PNR data to be processed, for example, for the purposes of improving external border controls or combatting illegal immigration, must be precluded.[218] The Court also stressed that the system set up by the PNR Directive could not be used to combat "ordinary crime", a matter of definition for each Member State.[219]

As concluded in *Opinion 1/15* and likewise in *Ligue des droits humains*, PNR data is considered limited enough to the specific context of air travel to not be capable of revealing such aspects of a person's private life that processing of PNR data would adversely affect the essence of the right to private life.[220] Although not allowing for a full overview of the person's private life, the enablement of setting up of a profile has been deemed equally serious as an interference with the essence.[221] In *Ligue des droits humains* the Court declared that an interpretation of the PNR Directive allowing for the matching of PNR data against "relevant databases" and thus the establishment of a detailed profile of an individual, was disproportionate since it could generate "in the minds of passengers… the feeling that their private life is under a form of surveillance".[222] The Court's rare statement that a provision of the PNR Directive was disproportionate thus had clear ties to the concept of essence.

The fact that purpose limitation, as constitutes the essence of Article 8 of the Charter, and the setting up of a profile, which is equally severe to an interference with the essence of Article 7 of the Charter, led to the Courts limiting interpretations thus shows tendencies towards a relative approach to the concept of essence. It supports the claim that essence, as suggested by

[216] Article 1(2) PNR Directive which reads as follows. "PNR data collected in accordance with this Directive may be processed only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime".

[217] Ligue des droits humains (not 17), para 233, 235 & 237.

[218] Ligue des droits humains (not 17), para 235 & 288–291.

[219] Ligue des droits humains (not 17), para 148–152. Although unable to itself specify what crimes amount to "serious crimes" with respect to each national criminal judicial systems, the Court held that crimes such as human trafficking, the sexual exploitation of children and child pornography, money laundering, cybercrime, murder, rape, kidnapping (etc., see para 149), are inherently and indisputably extremely serious.

[220] Opinion 1/15 (not 54), para 150–151; Ligue des droits humains (not 17), para 120.

[221] Tele2 Sverige and Others (not 58), para 99.

[222] Ligue des droits humains (not 17), para 184.

scholars, indicates that the proportionality analysis needs to be done more strictly, or that essence serves as a normative pivot.[223]

5.3 Proportionality after Case C-817/19

Under questions 2, 3, 4, and 6 the Court assessed the validity of the PNR Directive in light of the Charter right to data protection and carried out a proportionality analysis.[224] First, the Court stated the applicability of Articles 7 and 8 of the Charter and the existence of an interference with those rights.[225] It then examined the seriousness of those interferences, resulting in the following conclusion.

> In the light of all of the foregoing, it is appropriate to find that the PNR Directive entails undeniably serious interferences with the rights guaranteed in Articles 7 and 8 of the Charter, in so far, inter alia, as it seeks to introduce a surveillance regime that is continuous, untargeted and systematic, including the automated assessment of the personal data of everyone using air transport services.[226]

Two arguments leading to this conclusion were especially notable. Firstly, the fact that at least five out of six individuals were misidentified by the assessment carried out by means of automated processing.[227] Secondly, the fact that a very large part of the population of the EU is likely to constantly have their personal data retained and processed given that they travel by air at least once every five years.[228]

5.3.1 The Proper Purpose Sub-Test

The first step of the proportionality analysis, the proper purpose sub-test, is in *Ligue des droits humains* uncomplicated as it is settled that the objectives of combatting terrorist offences and serious crime are legitimate ends that meet the requirement. The Court upheld its previous case law and recalled that the objectives can justify even serious interferences with the rights enshrined in Articles 7 and 8 of the Charter.[229] The Court emphasized that particularly the prevention and punishment of terrorist offences "is of

[223] See Chapter 4.2.1 above.

[224] Ligue des droits humains (not 17), para 85 ff. Particularly paragraphs 12 & 18 of Annex I, and Articles 3(4) & 6 of the PNR Directive were examined.

[225] Ligue des droits humains (not 17), para 94–95, 97.

[226] Ligue des droits humains (not 17), para 111.

[227] Ligue des droits humains (not 17), para 106; Opinion of Advocate General Pitruzzella (not 135), para 78.

[228] Ligue des droits humains (not 17), para 110.

[229] Ligue des droits humains (not 17), para 122.

paramount interest for each Member State… to protect the essential functions of the State and the fundamental interests of society in order to safeguard national security".[230] The objective also satisfies principle of purpose limitation and legitimate basis enshrined in Article 8(2) of the Charter, thus justifying the processing of personal data without the data subject's consent.

5.3.2 The Suitability Sub-Test

The suitability, the second sub-test of the proportionality analysis, is met if the interfering measure (the processing of PNR data), is appropriate to achieve its goal (to protect the life and safety of persons and the internal security of the EU). The Court stated that

> the fairly substantial number of 'false positives'… limit the appropriateness of that system… [but] are not capable, however, of rendering the said system inappropriate for the purpose of contributing to the attainment of the objective of combating terrorist offences and serious crime.[231]

The Court thus upheld its preceding approach towards the suitability sub-test, considering the criterion satisfied as long as the measure is not directly *inappropriate* to attain its goal.[232] Rather it was enough that the measure *contributed* to the attainment of the objective.

After its judgement *Digital Rights Ireland*, the CJEU received criticism for not examining in more detail the appropriateness of data retention and processing as tools to combat serious crime.[233] The same could be claimed in *Ligue des droits humains*. As noted in the judgement, in 2018 and 2019 less than one out of six individual identified by automated processing using the system set up by the PNR Directive was a match when crosschecked by a human.[234] Brown and Korff are likely not to agree with the assessment made by the Court since they argue that mass surveillance for the purposes of identifying potential terrorists is unproportionate to the harm it causes.[235] The unavoidable misidentification caused by algorithmic false positives, they claim, often target members of minority groups which institutes discrimination and undermines democracy and the rule of law. They conclude that "[t]he European surveillance society is developing in a profoundly undemocratic way".[236]

[230] Ligue des droits humains (not 17), para 170. Italics added.
[231] Ligue des droits humains (not 17), para 123.
[232] Digital Rights Ireland and Others (not 48), para 50.
[233] Lynskey (not 11), 167.
[234] Ligue des droits humains (not 17), para 106.
[235] Brown, I., & Korff, D. (2009). Terrorism and the Proportionality of Internet Surveillance. *European Journal of Criminology*, 6(2), 119–134, 131.
[236] Brown & Korff (not 235), 131–132.

5.3.3 The Blurring of Sub-Tests

Having determined that the requirements of provided for by law (formality), respect for the essence, proper purpose, and suitability have been met, the Court judged on the remaining requirements together under the headline of "*Whether the interferences from the PNR Directive are necessary*".[237] The headline suggests that only the necessity of the interfering measure is being examined. However, as defined in doctrine and as follows from Article 52(1) of the Charter, the remaining requirements that need to be assessed are provided for by law (quality), necessity, and *stricto sensu* proportionality.

By not clearly examining the requirements separately, the CJEU is blurring aspects that would more appropriately be judged separately. In theory a clear division between the criteria as set out in Article 52(1) of the Charter can be established. In practice the CJEU possesses the authority to interpret EU legal acts, including the Charter, which follows from Article 19(1) TEU. The Court therefore has the competence to establish the principles and methods of its own interpretations of the Charter. It is the settled case law of the Court that the quality of the law is best assessed together with the proportionality.[238] The Court is not as transparent regarding its conjunct judging of necessity, the final step of the 'means-end analysis' and the final 'threshold requirement', and *stricto sensu* proportionality which is value-based and not a 'threshold requirement'. Such blurring of value-based and 'threshold requirements' has been criticized by scholars.[239]

5.3.4 The *Stricto Sensu* Proportionality Sub-Test

The Court's conclusion of the PNR Directive's validity did not involve a clear statement on whether the legislature has struck a fair balance between the competing interests, but rather emphasizes necessity. The Court may have reason to avoid a clear statement on the *stricto sensu* proportionality because of its moral and political nature and to avoid political controversies.[240] In doing so, however, it avoids to properly state whether the benefit of the interference compensates the harm.[241] The question the Court abstains from answering is if we are, as Brown and Korff argue, "giving up freedom without gaining in security".[242]

The Court only commented explicitly on *stircto sensu* proportionality, as mentioned above, in relation to the advanced assessment of PNR data by

[237] Ligue des droits humains (not 17), para 125 ff.
[238] See Chapter 4.1 above.
[239] Brkan (not 155), 875; Dalla Corte (not 28), 15.
[240] See Chapter 4.3.2 above.
[241] Dalla Corte (not 28), 12 & 15.
[242] Brown & Korff (not 235), 131–132.

matching it to 'relevant databases' which would allow for the establishment of a detailed profile of an individual's private life.[243] By interpreting the provisions in such a way that the term "relevant databases" was specified to include only those databases explicitly mentioned in the PNR Directive,[244] the Court, however, concluded that the provision was consistent with the Charter.[245]

The same conclusion was made in relation to processing of PNR data against pre-determined criteria, provided that the number of false positives is kept to a minimum, that any match is cross-checked by a human to verify it, that the assessment criteria are set in a non-discriminatory manner, and that the process is reviewed to exclude any discriminatory results.[246] The essence and contents of the fundamental right to protection of personal data is still being shaped and influenced in relation to the development of new technology. Data protection in relation to algorithmic decision making is one such aspect that is being negotiated in *Ligue des droits humains* and the judgement did in this instance hand down some clarity. The Court, however, set up a very complicated description of what an individual has the right to know regarding how a decision based on pre-determined criteria was made. The Court stated that

> the competent authorities must ensure that the person concerned – without necessarily allowing that person, during the administrative procedure, to become aware of the pre-determined assessment criteria and programs applying those criteria – is able to understand how those criteria and those programs work so that it is possible for that person to decide with full knowledge of the relevant facts whether or not to exercise his or her right to the judicial redress.[247]

A person should be able to make a decision 'with full knowledge' of the relevant facts and understand how the criteria work, but at the same time the person does not have a right to 'become aware' of what the pre-determined criteria are. There is seemingly a fine balance to strike between the persons *awareness* of the pre-determined criteria and their *understanding* of how those criteria work.

According to Rotenberg, the CJEU takes a stance on decisions made by artificial intelligence in line with the ELI Guiding Principles, and specifically the traceable decision (it must be possible to establish how a decision was

[243] Ligue des droits humains (not 17), para 184.

[244] Article 6(3)(a) of the PNR Directive allows for the comparison of PNR data against relevant databases "including databases on persons or objects sought or under alert, in accordance with [EU], international and national rules applicable to such databases".

[245] Ligue des droits humains (not 17), para 185–192.

[246] Ligue des droits humains (not 17), para 203 & 213.

[247] Ligue des droits humains (not 17), para 210.

made) and reasoned decision principles (a decision should not be arbitrary) can be traced in the Court's arguments.[248] Rotenberg seems to argue that the Court draws a hard line, or a "red line", at the use of opaque machine learning techniques relying on statistical inferences to make decisions about people. Such a decision risks interfering with the right to an effective judicial remedy. This hard line is drawn in accordance with the ELI Guiding Principles which are becoming international standard.[249]

Since the Court did not invalidate the PNR Directive it was unavoidably faced with the task to carry out a *stricto sensu* proportionality balancing. The balancing or valuing of the competing interests can be summarized in the Courts choice of wording regarding the harm caused by the interference, described as "undeniably serious" and the benefit of the interference, the interest of combatting of terrorist offences, being described as "paramount".[250] Although not making an explicit and clear statement on the matter, other than to some extent in relation to the automated processing of PNR data, in conclusion the Court decided that the *paramount* objective of protecting national security outweighed the *undeniably serious* interferences with the right to data protection.

5.4 Necessity after Case C-817/19

The concept of necessity functions to ensure that the interfering measure is "the least intrusive effective measure available to attain the objective pursued".[251] In its data protection jurisprudence, the CJEU has stressed that infringements may only apply in so far as is strictly necessary.[252]

5.4.1 Indiscriminate Application

Regarding the retention period, the Court upheld its previous case law stating that the indiscriminate retention of PNR data of all passengers for five years was not limited to what is strictly necessary and that the continued storage of PNR data after the initial six months could only be justified if there is objective evidence establishing a link, even an indirect one, to the purposes

[248] Rotenberg, M., "*The Law of Artificial Intelligence and the Protection of Fundamental Rights: The Role of the ELI Guiding Principles*" in European Law Institute (ELI) Newsletter (Issue 4: July–August 2022) <https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Newsletter/2022/Newsletter_Jul-Aug_2022.pdf> accessed 8 December 2022.

[249] Rotenberg (not 248). He also states the relation to the proposed AI directive.

[250] Ligue des droits humains (not 17), para 111 & 170.

[251] EDPS Guidelines (not 200), 12.

[252] See Chapter 4.3.3 above.

of combatting terrorist offences and serious crime and the carriage of the passenger by air.[253]

The Belgian legislature had implemented the PNR Directives Article 12(1) as allowing for all PNR data about all passengers to be retained for five years,[254] an interpretation that aligns well the wording of the provision.[255] Putting quite some emphasis on reading the provision 'in light of the Charter' and thus counter to its wording, the CJEU's interpretation of the provision was that PNR data *can* be retained for a maximum of five years, if strictly necessary. While precluding national legislation allowing for the indiscriminate retention of PNR data, the Court evidently adjusted the directive in a way not intended by the EU legislature. The interpretation leaves the decision of in what cases data can be retained for the full period of five years at the discretion of national actors, i.e. PIUs and national courts.

Although allowing for retention for the full period of five years, the disclosure of the full PNR data after the initial six months, in other words, the reidentification of a passenger after the data has been depersonalized, is permitted under the PNR Directive only when (1) there is reasonable belief that the identification of the person is necessary to combat terrorist offences and serious crime, and (2) the disclosure has been approved by *a judicial or other competent national authority* verifying that necessity.[256]

Belgian legislation implementing the provision above allowed the PIU, which collects and retains the PNR data, to also be considered 'another competent national authority' that authorizes such disclosure – an interpretation that the CJEU declared must be precluded.[257] As pointed out by the General Advocate in his opinion, the PIU could very well be made up of the same staff members as the requesting authority, emanating i.e. from the police, state security, general intelligence, or customs.[258] The Court stated that the requesting authority and the PIU therefore are "necessarily linked" and the PIU cannot be considered a neutral third party in relation to the authority requesting the disclosure of the data.[259]

[253] Ligue des droits humains (not 17), para 257–258 & 262.

[254] Ligue des droits humains (not18), para 248.

[255] Article 12(1) of the PNR Directive reads as follows. "Member States shall ensure that the PNR data provided by the air carriers to the PIU are retained in a database at the PIU for a period of five years after their transfer to the PIU of the Member State on whose territory the flight is landing or departing".

[256] Article 12(3) PNR Directive.

[257] Ligue des droits humains (not 17), para 247.

[258] Opinion of Advocate General Pitruzzella (not 135), para 271. The 'PIU' and the 'requesting authority' as defined in Articles 4(1) & 7(2) of the PNR Directive are both described as "[authority/ies] competent for the prevention, detection, investigation or prosecution of terrorist offences or serious crime".

[259] Ligue des droits humains (not 17), para 245.

By its judgement the CJEU thus provided clarity regarding the degree of independence required between national authorities that retain data, request and approve its disclosure. Although the retaining and requesting authorities may naturally be made up of the same staff members, the authority that can approve disclosure of depersonalized PNR data, and that is meant to act as the equivalent of judicial authority, must have a higher degree of independence to guarantee that the data subjects judicial rights are observed and to keep the PNR Directive limited to what is strictly necessary.[260]

The Court once again emphasized the concept of necessity regarding the application of the system set up by the PNR Directive to intra EU flights. The Court specified that Member States may select certain routes, travel patterns, or airports based on indications that the processing of PNR data is justified for those flights.[261] The indiscriminate application of the system set up by the PNR Directive to all intra EU-flights could however only be considered limited to what is strictly necessary when there are "sufficiently solid grounds for considering that the [Member State] is confronted with a terrorist threat which is shown to be genuine and present or foreseeable".[262] Notably the Court does not state that the indiscriminate application to all intra-EU flights would be disproportionate, but that it would not meet the requirement of necessity. Likewise, the application of the PNR Directive to all extra-EU flights did, according to the Court, "not go beyond what is strictly necessary" in contrast to a statement of the application being proportional.[263]

5.4.2 Clarity & Precision

In his opinion the Advocate General suggested that paragraph 12 of Annex I of the PNR Directive should be declared invalid since it included "general remarks" as a category of PNR data that PIUs could demand to access.[264] The Court found that even though "the phrase 'general remarks' does not meet the requirements of clarity and precision… the list in brackets does".[265] With reference to the general principle of interpretation the Court found that paragraph 12 of Annex I of the PNR Directive could therefore be interpreted in a way to render it conform with the provisions of the Charter by clarifying that the list in brackets was exhaustive and therefore sufficiently clear and precise.[266] The Court thus found a way to refine and adjust the provision by

[260] Ligue des droits humains (not 17), para 246.
[261] Ligue des droits humains (not 17), para 174.
[262] Ligue des droits humains (not 17), para 171 & 173.
[263] Ligue des droits humains (not 17), para 162.
[264] Opinion of Advocate General Pitruzzella (not 135), para 254.
[265] Ligue des droits humains (not 17), para 135. The list in brackets reads as follows "including all available information on unaccompanied minors under 18 years, such as name and gender of the minor, age, language(s) spoken, name and contact details of guardian on departure and relationship to the minor, name and contact details of guardian on arrival and relationship to the minor, departure and arrival agent".
[266] Ligue des droits humains (not 17), para 136 & 140.

reading it in light of the Charter and ensuring that it only applies in so far as is strictly necessary.

By emphasizing strict necessity and upholding its 'strictly necessary doctrine', the Court requires granularity regarding the limitation imposed by the interfering measure.[267] The requirement also relates to the quality of the law because the scope and application of a limitation must be provided for by the law that the limitations is based on.[268] The provided for by law requirement is an expression of the need for legal certainty.[269] The CJEU demonstrated a willingness to itself provide the required granularity, a task that arguably should have been fulfilled by the legislature and not the Court to fully meet the need for legal certainty. After *Ligue des droits humains* the restrictions to the limitations rather follow from the CJEU's case law and its interpretations of the PNR Directive than directly from the directive itself.

5.5 Data Protection & the Division of Powers

In exercising its mandate as a constitutional court, the role of the CJEU is to observe that the legislature has not exceeded its mandate and imposed norms that are incompatible with primary law. The depth and intensity of the judicial review of the CJEU can be summarized in the 'manifest test' meaning that the EU legislature enjoys a wide margin of discretion, particularly when the issue is politically or technically complex.[270] Particularly in relation to data protection, the CJEU might be hesitant to carry out an extensive judicial review because of its moral and political nature, the importance of data processing for the functioning of society, and the far-reaching societal implications its judgements can have.[271] For example, the Court's exercise of its powers in politically sensitive matters, such as the transborder flow of personal data ruled on in *Schrems II*, has been criticized by scholars.[272]

In his opinion, the Advocate General commented on the extent of the judicial review and held that it should be strict in light of the importance of fundamental rights, meaning that the discretion of the EU legislature therefore is reduced.[273] The Court did not follow the Advocate General's recommendation to partly annul the PNR Directive and thus carried out a less

[267] Dalla Corte (not 28), 11–12.
[268] See Chapter 4.1 above.
[269] See Chapter 4.1 above.
[270] Groussot X. & Petursson, G. T., "The EU Charter of Fundamental Rights Five Years on: The Emergence of a New Constitutional Framework?" in Vries, S. A. de, Bernitz, U., & Weatherill, S. (2015). *The EU Charter of Fundamental Rights as a binding instrument*, 147.
[271] Dalla Corte (not 28), 14 & 17.
[272] Groussot & Atik (not 56).
[273] Opinion of Advocate General Pitruzzella (not 135), para 109.

extensive judicial review in comparison to what the Advocate General suggested.

In *Germany v Parliament and Council*, a case unrelated to data protection, the Court declared that it was unable to partially annul a directive since that would entail an amendment of its provisions, a matter for the legislature.[274] Since the Court did not see an option to interpret the provisions of the directive in such a manner to render them in line with primary law in the case, it chose to fully invalidate the directive in order to respect the division of powers. In carrying out its judicial review the CJEU may test the legality but not expediency of an act, the proportionality analysis however inescapably subverts this division of powers.[275] A court upholding and protecting fundamental rights inevitably produces new law in doing so.[276] The legislative and judicial powers of the EU are thus acting in symbiosis, both contributing to the shaping of law which engages fundamental rights such as data protection legislation. This can create friction between the law as made by the Court in its judgements and secondary law as crafted by the EU legislature.

With regards to the general principle of interpretation, in *Ligue des droits humains* the Court appears unwilling to invalidate secondary law unless manifestly erroneous. In doing so the CJEU is indirectly weakening the scope of its judicial review reserving it for rare cases of severe interference. The appropriateness of the manifest test can be put into question, in particular when the review is taking place in light of fundamental rights.[277] Likewise the appropriateness of applying the general principle of interpretation in a case with such strong ties to human rights as *Ligue des droits humains* can be criticized. As pointed out by the Court itself, the PNR Directive entails "undeniably serious interferences with the rights guaranteed in Articles 7 and 8 of the Charter"[278] and affects "a very large part of the population of the European Union"[279].

The general principle of interpretation is an expression of the Courts respect for the separation of powers which is particularly important in politically sensitive matters such as questions engaging data protection and national security. The 'strictly necessary doctrine' on the other hand gives expression to the importance of safeguarding data protection as a constitutional right and to uphold the higher status of primary law by ensuring that limitations to the fundamental rights do not go beyond what is permissible by Article 52 of the Charter. In *Ligue des droits humains*, the general principle of interpretation

[274] Judgement of 5 October 2000, Germany v Parliament and Council, C-376/98, EU:C:2000:544, para 117.

[275] See Chapter 1.3.1 above.

[276] Stone Sweet & Mathews (not 30), 45.

[277] Groussot & Petursson (not 270), 148.

[278] Ligue des droits humains (not 17), para 111.

[279] Ligue des droits humains (not 17), para 110.

and the 'strictly necessary doctrine' are directly contradicting in terms of how extensive the judicial review, as carried out by the Court, should be.

In its efforts *not* to invalidate the PNR Directive, the Court allows itself a wide margin of interpretation to adjust the provisions, thus imposing on itself a legislative role, the appropriateness of which (although inevitable) can also be put into question with regards to respect of the division of powers. Judicial review by the CJEU resulting in the invalidation, or amendment of EU law puts pressure on the legislature to adapt to the Court's case law. As pointed out by Tracol, since the CJEU bases its judgements on the Charter right to data protection which is recognized as primary law, "EU secondary law adopted by the EU legislature should… be consistent with such case law and refrain from attempting to circumvent it".[280] Failure by the legislature to adapt to judgements of the CJEU thus results in the Court having to repeatedly strike down data protection legislation or preclude national legislation implementing it. Since the judgement of *Digital Rights Ireland* in 2014 the CJEU and the Member States have been "going around in circles" in terms of the Court invalidating EU legislation and precluding national legislation on the retention of and access to traffic and location data, and legislation that could "put a term to the dead end" remains, according to Tracol, nowhere in sight.[281]

Since the CJEU did not invalidate the PNR Directive, but rather made some slight amendments, seemingly a way has been found to avoid the cycle in relation to the retention of and access to PNR data, assuming that Member States will implement and enforce national legislation in accordance with the interpretations made in *Ligue des droits humains*. In its judgement the CJEU stressed that the Member States have an obligation to "ensure that they do not rely on an interpretation of the directive that would be in conflict with the fundamental rights" when implementing the PNR Directive,[282] an obligation the Court seems to rely heavily on. How well the Member States will follow the amendments to the PNR Directive as made by the Court, and its potential implications on future legislation regulating the use of PNR data remains to be seen.

[280] Tracol, X. (2023). The joined cases of Dwyer, SpaceNet and VD and SR before the European Court of Justice: The judgments of the Grand Chamber about data retention continue falling on deaf ears in Member States. *Computer Law and Security Review*, 48(2023, 105773), 14.

[281] Tracol (not 280), 14.

[282] Ligue des droits humains (not 17), para 87.

6 Conclusion

In this thesis, data protection has been examined as a constitutional right in the EU legal system. Data protection as a fundamental right and the conditions under which it can be limited have been described, *de lege lata*. Using a *de lege ferenda* approach, an examination of how well the judgement of the CJEU in *Ligue des droits humains* fits into this existing legal system was made, and in some instances the choices and interpretations made by the Court were criticized. This Chapter contains a summarizing discussion aimed at answering the research questions and offers some concluding remarks regarding how the fundamental right to data protection was enforced in *Ligue des droits humains*.

The European data protection regime centers the rights of individuals and is characterized by its clear ties to the fundamental rights to privacy and data protection as enshrined in Articles 7 and 8 of the Charter. The Charter has influenced secondary EU data protection law through the jurisprudence of the CJEU in exercising its mandate as a constitutional court. The Court has both invalidated secondary EU data protection law and amended it by its interpretations, declarations to which the EU legislature consequently has had to adapt to when adopting new data protection legislation. Because as stated by the EU legislature itself:

> In a society where individuals will generate ever increasing amounts of data, the way in which the data are collected and used must place the interests of the individual first, in accordance with European values, fundamental rights and rules.[283]

The right to protection of personal data can be limited when the criteria in Articles 8(2), (3), and 52 of the Charter are met. Any limitation must respect data protection principles such as purpose limitation, fairness, legitimate object, and legal basis, provide the data subject access to and rectification of their personal data, and institute an independent supervisory authority. The limitations must be provided for by law, the essence of the right must be respected, and any limitation may apply only in so far as it is strictly necessary. Subject to the principle of proportionality, the measure must pursue a proper purpose, be suitable, necessary and the benefit of the interference must be greater than the harm caused by the interference with the right.

The concepts of essence, proportionality, and necessity are especially relevant in *Ligue des droits humains*. The CJEU seemingly adopted an absolute approach towards the concept of essence, as had been suggested by the Advocate General in his opinion. Being a qualified right, the essence test

[283] European Commission (not 1), 1.

serves to ensure that a right, at the very least, is not completely abolished. The function of the concept of essence however remains unclear and the application of the general principle of interpretation seems to make the concept further relevant. Some of the Court's limiting interpretations, reading the PNR Directive 'in light of the Charter', had clear ties to the essence of the rights enshrined in Articles 7 and 8 of the Charter, as defined by the CJEU in its jurisprudence. A more relative approach to the function of essence can therefore be partially noted in *Ligue des droits humains* as the concept therein, to some degree, is intertwined with that of proportionality.

To an even further degree, the concepts of necessity and proportionality were blurred and connected in the judgement. Proportionality serves as a test (*lato sensu*) and as an act of balancing (*stricto sensu*). The interests that are balanced in the case, on the one hand, the right to data protection and, on the other hand, national security which serves to protect the life and safety of persons, are both important to individuals but by different means. Although not explicitly or openly stated by the Court, the interest of national security, firstly of combatting terrorist offences, and secondly serious crime, was favored over data protection since grave interferences with the rights enshrined in Articles 7 and 8 of the Charter were tolerated. The CJEU concluded that the PNR Directive lent itself to an interpretation that was consistent with primary law and came within the limits of what is strictly necessary.

The CJEU has heavily emphasized the concept of necessity in its data protection jurisprudence and continued to do so in *Ligue des droits humains*. In relation to the other requirements that need to be met in order to verify that an interference comes within the limits of Article 52(1) of the Charter, the CJEU put the most weight on necessity its judgement. Seemingly to a degree that if a provision is limited to what is strictly necessary, there is no need to verify the proportionality of the interference. By emphasizing strict necessity rather than proportionality, the Court seemingly avoided a value-based judgement of *if*, and in that case *how well*, the EU legislature, by adopting the PNR Directive, had struck a fair balance between the conflicting interests of data protection and national security.

The 'strictly necessary doctrine' imposes a requirement to in detail specify and constrain any interference with the right to protection of personal data. In light of these demands, the Court showed a willingness to itself refine and adjust the PNR Directive to render it in conformity with the Charter. The ambiguous definitions regarding what PNR data may be collected, the purposes for processing, the application of the PNR Directive to intra-EU flights, the advanced assessment of PNR data by automated processing, the databases against which PNR data can be matched, and the definition of independence between the PIU and the authority to which it discloses data, were all commented on and clarified in the judgement. Since interpretations

relying on the wording of the PNR Directive alone were not limiting its interferences to the strictly necessary, and in some instances were unproportionate according to the CJEU, it was faced with the decision to either invalidate the PNR Directive or to specify which interpretation of the wording that was the correct one reading the provision 'in light of the Charter'.

After *Ligue des droits humains*, the CJEU has strengthened its own mandate to co-legislate together with the EU legislator. The limitations to the PNR Directive follow, not only from the directive itself, but from the case law of the Court, something which negatively affects legal certainty. In doing so the Court is 'reading in-between the lines' of the PNR Directive and relying heavily on the Member States' legislature to do the same when implementing said directive. The general principle of interpretation thus serves as a justification for the Court to act in a legislative capacity in the name of avoiding to invalidate the PNR Directive. Having gone to considerable length making sure that the interference is limited to the strictly necessary, the CJEU has interfered with the choices made by the EU legislature, and by extension the people it represents. In another sense the Court prioritized to exhibit loyalty to the EU legislature by not invalidating the directive, but at the cost of taking on a lawmaking role itself.

The Charter provides a baseline of protection for individuals as they come in contact with technology. Because of the societal benefits of data processing, the fundamental right to protection of personal data is a right that inherently needs to be limited. The role of the CJEU is to ensure that such limitations are proportionate by enforcing the Charter. When rights are interfered with by the EU legislature, the Court can either invalidate secondary law, acting in its judicial capacity, or amend it, thus taking on a legislative role. According to the division of powers, the CJEU is however a judicial and not a legislative body.

The judgement *Ligue des droits humains* reveals a battle, not only between the competing interests of data protection and national security, but between the CJEU acting in its capacity as a constitutional court upholding fundamental rights and the EU legislature trying to impose limitations to these. Although national security arguably won the battle with data protection in *Ligue des droits humains*, the battle between the CJEU and the EU legislature has not been settled.

Bibliography

Literature

Bernitz, U., & Kjellgren, A. (2022). *Europarättens grunder (Sjunde upplagan).* Norstedts juridik.

Brkan, M. (2019). The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning. *German Law Journal*, 20(6), 864–883.

Brown, I., & Korff, D. (2009). Terrorism and the Proportionality of Internet Surveillance. *European Journal of Criminology*, 6(2), 119–134.

Bygrave, L. A. (2002). *Data protection law : approaching its rationale, logic and limits.* Kluwer.

Bygrave, L. A. (2014). *Data privacy law : an international perspective.* Oxford University Press.

Bygrave, Lee A. (2021) The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects. *Computer Law & Security Review,* 40(April 2021, 105460), 1–13.

Dalla Corte, L. (2022). On proportionality in the data protection jurisprudence of the CJEU. *International Data Privacy Law*, 12(4), 259–275.

González Fuster, G., & Gutwirth, S. (2013). Opening up personal data protection: A conceptual controversy. *Computer Law & Security Review*, 29(5), 531–539.

Greenstein, S. (2017). *Our humanity exposed : predictive modelling in a legal context.* Department of Law, Stockholm University.

Groussot X. & Petursson, G. T. (2015), "The EU Charter of Fundamental Rights Five Years on: The Emergence of a New Constitutional Framework?" in Vries, S. A. de, Bernitz, U., & Weatherill, S. (eds.). *The EU Charter of Fundamental Rights as a binding instrument. five years old and growing.* Hart Publishing.

Groussot, X., & Atik, J. (2021). A Weaponized Court of Justice in Schrems II. *Nordic Journal of European Law*, 4(2), 1–21.

Groussot, X., & Petursson, G. T. (2022). Je t'Aime... Moi Non plus: Ten Years of Application of the EU Charter of Fundamental Rights. *Common Market Law Review,* 59(1), 239–258.

Hallinan, D. (2021). The Essence of Data Protection: Essence as a Normative Pivot. *European Journal of Law & Technology*, 12(3), 57–80.

Lebeck, C. (2016). *EU-stadgan om grundläggande rättigheter (2., [rev.] uppl.).* Studentlitteratur.

Lenaerts, K. (2019). Limits on Limitations: The Essence of Fundamental Rights in the EU. *German Law Journal*, 20(6), 779–793.

Lindroos-Hovinheimo, S. (2022). Individualism eller sammanflätade liv? En undersökning av integritetsskyddets filosofiska grundvalar, *Europarättslig tidskrift*, 25(1), 59–74.

Lynskey, O. (2015). *The foundations of EU data protection law (1st edition.).* Oxford University Press.

Lynskey, O. (2020), "Article 8: The Right to Data Protection." in Bobek, M., & Prassl, J. (eds.). *The EU charter of fundamental rights in the member states.* Hart Publishing, an imprint of Bloomsbury Publishing.

Reichel, J. (2018) "EU-rättslig metod." in Nääv, M. & Zamboni, M. (eds.). *Juridisk metodlära (Andra upplagan).* Studentlitteratur.

Rotenberg, M., "*The Law of Artificial Intelligence and the Protection of Fundamental Rights: The Role of the ELI Guiding Principles"* in European Law Institute (ELI) Newsletter (Issue 4: July–August 2022) <https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Newsletter/2022/Newsletter_Jul-Aug_2022.pdf> accessed 8 December 2022.

Stone Sweet, A., & Mathews, J. (2019). *Proportionality Balancing and Constitutional Governance : A Comparative and Global Approach.* Oxford University Press.

Smits, J. M. (2017), "What is legal doctrine?: On the aims and methods of legal-dogmatic research." in Van Gestel, R., Micklitz, H.-W., & Rubin, E. L. (eds.). *Rethinking legal scholarship: A transatlantic dialogue.* Cambridge University Press.

Tracol, X. (2023). The joined cases of Dwyer, SpaceNet and VD and SR before the European Court of Justice: The judgments of the Grand Chamber about data retention continue falling on deaf ears in Member States. *Computer Law and Security Review*, 48(2023, 105773), 1–14.

Yeung, K. (1), & Bygrave, L. A. (2). (2022). Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. *Regulation and Governance*, 16(1), 137–155.

Young, A. L. & Búrca, G. (2017)," Proportionality." in Vogenauer, S., & Weatherill, S. (eds.). *General principles of law. European and comparative perspectives.* Hart Publishing.

Zuboff, S. (2019). *The age of surveillance capitalism : the fight for the future at the new frontier of power.* Profile Books.

Åhman, K. (2019). *Grundläggande rättigheter och juridisk metod : RF 2 kap., Europakonventionen och EU:s stadga och deras tillämpning (Andra upplagan).* Norstedts juridik.

EU Sources

European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions, *A European strategy for data"* COM (2020) 66 final.

European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions, *Shaping Europe's digital future***"** COM (2020) 67 final.

European Data Protection Supervisor, "*EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*" (25 February 2019) <https://edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf > accessed 22 October 2022.

Council of Europe Website

Council of Europe, "Data Protection; Convention 108 and Protocols; Parties – *Convention 108 in the World"* <https://www.coe.int/en/web/data-protection/convention108/parties> accessed 2 December 2022.

Council of Europe, "Treaty Office; Full list – *Chart of signatures and ratifications of Treaty 005"* <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=005> accessed 2 December 2022.

Table of Cases

CJEU Cases

Judgment of 13 December 1983, Commission v Council, C-218/82, ECR 4063.

Judgment of 12 November 1996, United Kingdom v Council, C-84/94, EU:C:1996:431.

Judgement of 5 October 2000, Germany v Parliament and Council, C-376/98, EU:C:2000:544.

Judgement of 29 January 2008, Promusicae, C-275/06, EU:C:2008:54.

Judgement of 7 May 2009, Rijkeboer, C-553/07, EU:C:2009:293.

Judgement of 9 November 2010, Volker und Markus Schecke and Eifert v Land Hessen, C-92/09 and C-93/0, EU:C:2010:662.

Judgement of 31 January 2013, McDonagh, C-12/11, EU:C:2013:43.

Judgement of 19 September 2013, Review of Commission v Strack, C-579/12 RX-II, EU:C:2013:570.

Judgement of 7 November 2013, IPI, C-473/12, EU:C:2013:715.

Judgement of 8 April 2014, Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238.

Judgement of 6 October 2015, Schrems, C-362/14, EU:C:2015:650.

Judgment of 15 February 2016, N., C-601/15 PPU, EU:C:2016:84.

Judgement of 21 December 2016, Tele2 Sverige and Others, C-203/15 and C-698/15, EU:C:2016:970.

Opinion of 26 July 2017, Opinion 1/15 Accord PNR EU-Canada, EU:C:2017:592.

Judgement of 14 May 2019, M and Others, C-391/16, C-77/17 and C-78/17, EU:C:2019:403.

Judgement of 16 July 2020, Facebook Ireland and Schrems, C-311/18, EU:C:2020:559.

Judgement of 6 October 2020, Privacy International, C-623/17, EU:C:2020:790.

Judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791.

Judgment of 2 February 2021, Consob, C-481/19, EU:C:2021:84.

Opinion of Advocate General Pitruzzella delivered on 27 January 2022, Ligue des droits humains, C-817/19, EU:C:2022:65.

Judgement of 5 April 2022, Commissioner of An Garda Síochána, C-140/20, EU:C:2022:258.

Judgement of 21 June 2022, Ligue des droits humains, C-817/19, EU:C:2022:491.

Judgement of 20 September 2022, SpaceNet, C-793/19 and C-794/19, EU:C:2022:702.

Judgement of 20 September 2022, VD and SR, C-339/20 and C-397/20, EU:C:2022:703.

ECtHR Cases

Amann v. Switzerland [GC], App no 27798/95, ECHR 2000-II.

Rotaru v. Romania [GC], App no 28341/95, ECHR 2000-V.

Big Brother Watch and Others v. the United Kingdom [GC], App nos 58170/13, 62322/14 and 24960/15, 25 May 2021.