

Hello. It's me.

The invisible journey and uncertain validity of Passenger
Name Records

Ricardo Rodrigues de Oliveira

Thesis submitted for assessment with a view to obtaining
the degree of Doctor of Laws of the European University Institute

Florence, 22 November 2021

European University Institute
Department of Law

Hello. It's me.

The invisible journey and uncertain validity of Passenger Name Records

Ricardo Rodrigues de Oliveira

Thesis submitted for assessment with a view to obtaining
the degree of Doctor of Laws of the European University Institute

Examining Board

Professor Albertina Albors-Llorens, Cambridge University
Professor Deirdre Curtin, European University Institute
Professor Valsamis Mitsilegas, Queen Mary University of London
Professor Joanne Scott, European University Institute (supervisor)

© Ricardo Rodrigues de Oliveira, 2021

No part of this thesis may be copied, reproduced or transmitted without prior
permission of the author

**Researcher declaration to accompany the submission of written work
Department of Law – LL.M. and Ph.D. Programmes**

I Ricardo Filipe Rodrigues de Oliveira certify that I am the author of the work “Hello. It’s me. The invisible journey and uncertain validity of Passenger Name Records” I have presented for examination for the Ph.D. at the European University Institute. I also certify that this is solely my own original work, other than where I have clearly indicated, in this declaration and in the thesis, that it is the work of others.

I warrant that I have obtained all the permissions required for using any material from other copyrighted publications.

I certify that this work complies with the Code of Ethics in Academic Research issued by the European University Institute (IUE 332/2/10 (CA 297)).

The copyright of this work rests with its author. Quotation from this thesis is permitted, provided that full acknowledgement is made. This work may not be reproduced without my prior written consent. This authorisation does not, to the best of my knowledge, infringe the rights of any third party.

I declare that this work consists of 113 887 words.

Statement of language correction:

This thesis has been corrected for linguistic and stylistic errors.

I certify that I have checked and approved all language corrections, and that these have not affected the content of this work.

Signature and date:

14 September 2021

A handwritten signature in black ink, appearing to read 'Ricardo Filipe Rodrigues de Oliveira', written in a cursive style.

Summary

With the approval of Directive (EU) 2016/681 on the use of Passenger Name Records (PNR), the personal information provided to carriers by air passengers crossing European Union (EU) borders is available for mining by national law enforcement, third countries, and Europol. This is in line with other pre-emptive security policies, but it goes further in generalizing suspicion over large numbers of EU and non-EU travelers.

After years of pressure from the United States under the banner of the global war on terror, air companies are no longer between a rock and a hard place. They are now able to lawfully disclose big data gathered as part of the normal course of business. Following booking and reservation, up to 19 items of individual data must be provided to Passenger Information Units for criminal investigations and other appropriate actions.

The intra-EU PNR system has managed to fly under the radar of scholars and public opinion. Most specialized literature is limited to superficial discussions on security and privacy. There is insufficient research looking at it comprehensively and in detail.

This thesis explores this novel security policy in depth and questions its validity. It argues that the PNR scheme should be invalidated by the Court of Justice of the EU for two reasons. In the first place, the Union was not competent to approve a secondary law so intrusive to the national security agendas and policies of the member states. Secondly, the Directive disproportionately encroaches upon the fundamental rights of passengers.

There is, as yet, no doctoral project which analyzes the EU PNR so thoroughly. This work fills a gap in scholarly writing regarding fundamental rights and creeping competences in EU law. Its novelty lies in questioning issues that have been overlooked, or insufficiently addressed, in the journey of the PNR Directive.

Table of Contents

Summary i
Table of contents ii
Abbreviations x
Acknowledgments xii

Introduction 1
 1. Subject matter and research question 1
 2. Methodology 3
 3. Limitations 6
 4. Structure of the study 7

Chapter 1.
An aviation story

Introduction 9
1. Check-in 10
 1.1 A broader context 10
 1.2 Booking and ticketing 12
 1.3 Transferring basic personal data 14
2. Working definitions 15
3. Flying abroad 17
 3.1 United States of America 17
 3.2 Canada 22
 3.3 Australia 25
 3.4 Prospective agreements and a revised global approach 26
4. A long departure 29
 4.1 Harmonizing the common space 30
 4.2 Transposing the Directive 33
 4.3 The 2020 review 36

Chapter 2.

Creeping competences: A (not so) clear runway

Introduction	37
1. Reviewing the legal bases	38
1.1 Article 82(1)(d) TFEU	39
1.2 Article 87(2)(a) TFEU	42
1.3 The missing Article 16 TFEU	45
2. Limits to competence creep	49
2.1 A long story short	49
2.2 The Lisbon <i>status quo</i> on security	51
2.3 Applicable national security exceptions	53
2.3.1 Article 72 TFEU	57
A. Defining internal security	58
B. Weakened provision	60
C. Insufficient basis to prevent creeping competences	62
2.3.2 Article 4(2) TEU, <i>in fine</i>	63
A. Difficult interpretation	66
A.1 National security	66
A.2 Sole responsibility	73
B. PNR beyond conferral	78

Chapter 3.1

Trumping fundamental rights: Departure

Introduction	83
1. Reviewing the literature	84
1.1 Security, privacy, and data protection	85
1.1.1 Tension and trade-off	86
1.1.2 A necessary tool	87
A. Common instruments for EU security	87
B. Mechanisms of data protection	88
C. Data retention period	90
1.1.3 Insufficient guarantees	91

A. Data retention period	91
B. Third parties with access rights	92
1.2 Profiling and discrimination	93
1.2.1 Modern profiling techniques	94
1.2.2 A necessary tool	95
1.2.3 Unlawful profiling and discrimination	95
A. Operational errors and incorrect predictive assessments	96
B. Negative discrimination	97
1.3 Data rights and transparency	99
1.3.1 Sufficient guarantees	99
1.3.2 Insufficient protection	100
2. In the legislative process	103
2.1 National contributions	104
2.1.1 Tension and trade-off	105
2.1.2 Data retention period	105
2.1.3 Profiling and discrimination	106
2.1.4 Right to notification	106
2.2 Input from auxiliary and supervisory entities	106
2.2.1 Committee of the Regions	107
2.2.2 European Data Protection Supervisor	107
A. Harmonized system	108
B. Impact assessments	108
C. Data retention period	109
D. Transparency	109
2.2.3 European Economic and Social Committee	109
2.3 The debate in the European Parliament	111
2.3.1 The kick-off	111
2.3.2 Tension and trade-off	111
A. For security	112
B. For privacy and data protection	113
2.3.3 Data rights and transparency	115
2.3.4 Wrapping-up	115

Introduction	119
1. Joined cases C-293/12 and C-594/12	122
1.1 Serious interference	124
1.1.1 Was there an interference?	124
1.1.2 When did the interference take place?	127
1.1.3 Was the interference serious?	127
1.2 Provided for by law	129
1.3 The essence of the rights	130
1.3.1 To privacy	130
1.3.2 To data protection	131
1.4 Objectives of general interest recognized by the EU	131
1.5 The principle of proportionality	132
1.5.1 Adequacy	133
1.5.2 Strict necessity	134
A. Quantity of collected data	135
B. Data retention period	136
C. Third parties with access rights	137
C.1 Public entities	137
C.2 Private actors	139
C.2.1 Level of protection	139
C.2.2 Processing overseas	141
1.6 Relevant takeaways	141
2. Opinion 1/15	142
2.1 Serious interference	144
2.1.1 Was there an interference?	144
2.1.2 When did the interference take place?	145
2.1.3 Was the interference serious?	145
2.2 Provided for by law	147
2.3 The essence of the rights	147
2.3.1 To privacy	147
2.3.2 To data protection	148

2.4 Objectives of general interest recognized by the EU	148
2.5 The principle of proportionality	149
2.5.1 Adequacy	149
2.5.2 Strict necessity	150
A. Quantity and quality of collected data	150
A.1 A matter of quantity	151
A.2 A matter of quality	152
B. Data retention period	153
C. Third parties with access rights	155
2.6 Right to notification	155
2.7 Relevant takeaways	158

Chapter 3.3

Trumping fundamental rights: Arrival

Introduction	161
1. The scope and content of fundamental rights	163
1.1 To privacy	164
1.2 To data protection	165
2. Serious interference	167
2.1 Is there an interference?	167
2.2 When does the interference take place?	171
2.3 Is the interference serious?	172
2.3.1 Systemic indifference	172
2.3.2 A recent red line	175
3. Provided for by law	176
4. The essence of the rights	177
4.1 To privacy	177
4.2 To data protection	179
5. Objectives of general interest recognized by the EU	183
6. The principle of proportionality	186
6.1 Adequacy	187
6.2 Strict necessity	188
6.2.1 Quantity and quality of collected data	189

A. A matter of quantity	189
A.1 The amount of collected data	189
A.2 Legal uncertainty	193
B. A matter of quality	195
6.2.2 Data retention period	197
A. Objective criteria	198
B. Categories of data and relevance of passengers	199
C. Irreversible destruction of data	202
D. Reasonable limitation	204
D.1 Depersonalization mechanisms	207
D.2 Renewal of PNR receipts	209
D.2.1 First chilling effect	209
D.2.2 Second chilling effect	210
D.2.3 Third chilling effect	211
6.2.3 Third parties with access rights	213
A. Public entities	213
A.1 Competent authorities	213
A.1.1 A broader concern	214
A.1.2 Opening of the system	216
A.1.3 Authorized personnel	218
A.1.4 Prior review	219
i) Moment of review	220
ii) Competent authorities	222
A.2 Third countries	223
B. Private actors	225
B.1 Economic considerations	226
B.2 Irreversible destruction of data	227
7. Right to notification	229
8. Closing remarks	231
Conclusions	233
1. Main findings	233
2. Broader lessons	238
2.1 A poisoned package	238

2.2 Demonstration effects	239
2.3 Contingent unilateralism and hypocrisy	243
2.4 Effectiveness reports	245
Annex: References	251
A. Legislation and policy documents	251
1. Council of Europe	251
2. EU	251
2.1 Primary law	251
2.2 Secondary law	251
2.2.1 Commission	251
2.2.2 Council	253
2.2.3 Council of the EU	253
2.2.4 European Council	255
2.2.5 European Parliament	255
2.2.6 Multiple institutions	257
i) Directives	257
ii) Regulations	258
2.2.7 Other	258
3. International agreements and policy	259
4. International Air Transport Association	260
5. International Civil Aviation Organization	260
6. Member states of the EU	260
6.1 Austria	260
6.2 Germany	260
6.3 The Netherlands	260
7. Third countries	261
7.1 Australia	261
7.2 Canada	261
7.3 United States of America	261
B. Cases and opinions	262
1. European Court of Human Rights	262
2. Court of Justice of the EU	262
3. Other courts	268

- C. Opinions from advisory and supervisory bodies of the EU 268**
 - 1. The Article 29 Working Party 268**
 - 2. Committee of the Regions 270**
 - 3. European Data Protection Supervisor 270**
 - 4. European Economic and Social Committee 271**
 - 5. Fundamental Rights Agency 271**
- D. Bibliography 273**

Abbreviations

AFSJ	Area of Freedom, Security and Justice
AG	Advocate General
ALDE	European Party Alliance of Liberals and Democrats for Europe at the European Parliament
API	Advance Passenger Information
CBSA	Canada Border Services Agency
CoE	Council of Europe
CFREU	Charter of Fundamental Rights of the European Union
CIVEX	Commission for Citizenship, Governance, Institutional and External Affairs of the Committee of the Regions of the European Union
CJEU	Court of Justice of the European Union
COR	Committee of the Regions of the European Union
CRS	Computerized Reservation System
DHS	Department of Homeland Security of the United States of America
DPO	Data Protection Officer
ECtHR	European Court of Human Rights
ECR	European Conservatives and Reformists Group at the European Parliament
EDPS	European Data Protection Supervisor
EESC	European Economic and Social Committee
EFA	European Free Alliance at the European Parliament
EFDD	Europe of Freedom and Direct Democracy at the European Parliament
EP	European Parliament

EPP	European People’s Party at the European Parliament
EU	European Union
FRA	European Union Agency for Fundamental Rights
GDPR	General Data Protection Regulation
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
IWG-PNR	European Informal Working Group on PNR
LIBE	Committee on Civil Liberties, Justice and Home Affairs of the European Parliament
MEP	Member of the European Parliament
OJ	European Union’s Official Journal
PIU	Passenger Information Unit
PNR	Passenger Name Records
S&D	Group of the Progressive Alliance of Socialists and Democrats at the European Parliament
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
US	United States of America

Acknowledgments

The first note of appreciation goes to my family and friends, both old and new. Doing a Ph.D. at the EUI is far more than enjoying the sunny slopes of Tuscany and they were always keen to know more about my research and to support my project. We have ached and laughed together and it seems we have made it through. I must thank particularly Sara Athouguia, without whom I would certainly not have managed. She was my rock during these years and I cannot imagine my present, or future, life without her.

I must likewise thank my current supervisor, professor Joanne Scott, and my former supervisor, professor Deirdre Curtin. They have helped shape what is now this work and I have grown immensely under their guidance. Professor Gábor Halmai was a supporting hand in more troubled times and I hope to meet him and his lovely wife, Marianna Török, again in the future, either in academia or swimming lessons. A word of gratitude goes also to the external examiners of my thesis, professors Albertina Albors-Llorens and Valsamis Mitsilegas, and to all other scholars I have encountered along the way. Some have provided me with in-depth comments, others with a practical angle, a broader gaze, or simply a pat on the back. Francesca Galli was always there to chat, while David Fennelly helped me pinpoint the crucial issues to discuss about PNR. And I cannot forget about Elif Kuskonmaz and Julie Hornle for their kindness and for including me in many projects, whereby I came across amazing professionals in London and Paris.

I also want to recall those whom I have met in other activities at the EUI and who made my journey so much nicer. Silke Tork has made me fond of the German language, as well as the German people (this time, it is not “sad, so sad”). She was a breath of fresh air, just like Edurne Iraiñoz and “la gente mayor” in her Spanish classes. I will forever cherish the thought that I was her little prince. They have both taught me so much. Nicola Hargreaves (aka Nicki) was always ready to help me with my texts and I must thank her specially for being the model of a kind and attentive teacher that I want to be. Teaching the Australian students at Monash University was a success and I could not have made it without her. Thank you too to the corrector of this thesis, Natasha Marhia, for the final touch.

A final grazie goes to all those in and outside the EUI who made my stay in Florence a unique adventure. I shall never forget my friends from the orchestra at the Scuola di Musica di Fiesole and those from water polo at Bellariva. *E come 'l volger del ciel de la luna cuopre e discuopre i liti senza posa, così fa di Fiorenza la Fortuna.*

Introduction

“National security concerns are also resulting in the widening of access to existing and future EU-wide databases (such as EURODAC, SIS and VIS), which will allow immigration data to be used for law enforcement purposes. There is something eerie in the prospect that the data of millions of visa applicants, and arguably their sponsors, will be accessible to law enforcement agencies, as if third country nationals were a specific category of suspect individuals.”¹

1. Subject matter and research question

This work is entitled ‘Hello. It’s me. The invisible journey and uncertain validity of Passenger Name Records.’ It is inspired by the opening lyrics of the song ‘Hello’ from the 2015 album ‘25’ by the British singer Adele. She sings “Hello, it’s me / I was wondering if after all these years you’d like to meet / To go over everything / They say that time’s supposed to heal ya, but I ain’t done much healing.”²

This research is not on copyright, or patent law. It is, instead, about a piece of pervasive security legislation that failed to gain approval when it was first put forward due to the problems it presented regarding fundamental rights. Time passed, there were many discussions, and this legislation ended up being sanctioned. Yet, time did not manage to heal the wounds it opened for the privacy and data protection of European citizens.

The European Union (EU) lived under a climate of fear in 2015 and 2016. A series of terrorist attacks within its borders led it to raise its security levels to an unprecedented degree. The Union and national legislators then set out to adjust their security agendas to better prevent, detect, investigate, and prosecute terrorism and serious crime. This led to the approval of wide-scope surveillance mechanisms that rely on the collection, retention, and processing of big data of a personal nature. Biometric, financial, and travel information are nowadays gathered to monitor EU citizens and third-country nationals in a systemic and systematic way, by public entities and private actors alike.

The legislation studied here was tabled for the first time in 2011 but only managed to achieve approval in 2016. On 27 April, the EU enacted Directive (EU) 2016/681, on Passenger Name Records (PNR).³ PNR refers to electronic receipts containing up to 19 elements of personal

¹ Baldaccini & Toner, 2007: 14.

² Adele, 2015.

³ 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 (Official Journal [OJ] L 119, 4.5.2016).

data of prospective air passengers. This information is inserted into booking and reservation systems. With this Directive, these data, which were once used exclusively by carriers for marketing and other private ends, must now be transferred to Passenger Information Units (PIUs), law enforcement authorities which process them to find meaningful patterns and connections to help fight terrorism and other serious crimes. PIUs can then transfer these data, or the results of their processing, to other authorities and agencies for further action.

This system reconfigures air security, permitting authorities to access data from passengers crossing EU borders almost instantaneously. It is a tool for police and judicial cooperation in the Area of Freedom, Security and Justice (AFSJ) that is more sophisticated than any of the previous data-based air security mechanisms.

PNR was approved together with the General Data Protection Regulation (GDPR).⁴ The contemporaneous climate of fear managed to hide PNR's flaws. In fact, the journey of the intra-EU PNR has been largely invisible to the public. There is a significant media gap between the GDPR and PNR. Most passengers, even frequent flyers, are not aware of the use that law enforcement can make of their data. This is, perhaps, why there was little commotion about a security policy that is so intrusive and ubiquitous. Its approval in 2016, without revising key aspects included in the 2011 draft which threaten privacy, data protection, and other fundamental values enshrined in EU primary law, might suggest that the Union is loosening its emphasis on privacy in favor of security.

Yet, as Anneliese Baldaccini and Helen Toner put it, if there is something eerie about making the data of millions of third country nationals available to law enforcement agencies when they cross EU borders, extending this to European citizens is even eerier. This research questions the validity of the 2016 intra-EU PNR scheme.⁵ Is Directive (EU) 2016/681 valid, and was the Union competent to approve it? These are the research questions that this thesis tries to answer. It argues that the PNR Directive should be declared invalid by the Court of Justice of the EU (CJEU) for two principal reasons. Firstly, the Union was not competent to approve the Directive as it did. It is so invasive to the national security agendas and policies of the member states that its adoption should have been voluntary, and the issues arising should have remained partially

⁴ 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) (OJ L 119, 4.5.2016).

⁵ 'Validity' is the term used in the context of preliminary ruling procedures. It will be used here instead of 'legality' since this is used regarding direct actions for annulment, which can only be tabled in the strict time limit of two months following publication, as set out in Article 263 of the Treaty on the Functioning of the EU (TFEU).

the responsibility of the member states, under the terms of the treaties.⁶ Secondly, the PNR scheme encroaches upon the fundamental rights of passengers in a disproportionate manner, thus violating the Charter of Fundamental Rights of the EU (CFREU).⁷

2. Methodology

This work combines an expository perspective and a normative perspective on the intra-EU PNR system. The expository aspect is present in the detailing of the evolution of this policy in Europe. It discusses its context, related instruments, the Union's external agreements for the transfer of data, and its internal development. Other examples of this approach can be seen in the review of the literature, parliamentary discussions, and opinions of supervisory bodies. The case law of the CJEU is also described. The exposition included in this thesis has been built on an exhaustive study of legal, policy, and jurisprudential material. Secondary sources were also essential, from academic articles and books to reports and information available online.

Exchanges of emails and conversations with experts, inside and outside academia, have been useful to comprehend the complexity of PNR. There are, nonetheless, no interviews mentioned in this work, or direct quotes from people who have assisted in the research. The insights offered by these interviews were used to highlight issues and questions that were addressed by reference to the documentary sources stressed above.

The normative perspective is legal and doctrinal in nature. It focuses on the unveiling of key problems that the approved Directive presents to the principle of conferral and the balance of shared competences in the AFSJ, as well as to the integrity of the fundamental rights of citizens. This project makes a legal claim about the validity of EU secondary law, searching for the limits of Union creeping competences and the lawfulness of provisions that curtail fundamental rights.

The legal analysis on fundamental rights is grounded in the literature review and the appraisal of the debates taking place at the European Parliament (EP) during the legislative process. Substantial insights are likewise gleaned from two recent decisions of the CJEU. This methodological approach, which combines these different sources and approaches (expository and normative/doctrinal), goes beyond existing studies on PNR.

There is already relevant literature exploring PNR and fundamental rights. Names like Cristina Casagran, Paul De Hert, Olga Enerstvedt, Mireille Hildebrant, Emmanuelle Saulnier-

⁶ Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (OJ C 306, 17.12.2007).

⁷ Charter of Fundamental Rights of the European Union (OJ C 326, 26.10.2012).

Cassia, Maria Tzanou, or Susanna Villani have made an enormous contribution to PNR, the AFSJ, and EU criminal and data protection laws. They, and many others, have been essential in moving this project forward. Yet, existing literature is insufficient on two accounts.

On the one hand, no previous study has examined the 2016 PNR in such a comprehensive and complete manner. There has been, so far, no analysis putting together a detailed account of this instrument's context and storyline with a methodical and substantive assessment of key issues. The literature review shows that some authors do explore the evolution of PNR but they do not discuss its features in depth. Others prefer to focus only on certain aspects, thus not considering its broad rationale, or background. Either way, there is a sense that the literature sees PNR as taking a back seat in relation to other security policies in the overall AFSJ. In fact, many authors only study it *à propos* other policies on crime and counter-terrorism.

That is the main reason this research focuses exclusively on the intra-EU PNR. There was a need to address this topic specifically, setting aside discussions about other security policies. The current literature has been crucial in identifying key problems with PNR, as a point of departure, but this analysis goes one step further.

On the other hand, most works do not critically discuss the published version of the Directive and consider the arguments that might render it susceptible to being invalidated by the Court. Few authors suggest how it could be improved, or amended, to comply with treaty law and the CFREU. This project does that in a clear way, thereby providing a concrete added value.

This added value also stems from assessing the debates in the EP. No scholar has looked closely at the concerns of the Members of the EP (MEPs) expressed in the final stages of the legislative process. Yet, the PNR Directive was far from gaining unanimous support in the debates. Many MEPs have tabled relevant arguments that can be used to criticize the validity of its provisions. These commentaries complement the opinions of scholars, making the doctrinal claim of this thesis more robust and ample.

Regarding the jurisprudence of the CJEU, there is already a relevant collection of cases mentioned in scholarly writing which illustrates the Court's position on privacy, data protection, security, and data rights. The case law serves two main purposes here.

First, it provides the formal structure to assess the validity of the PNR Directive. As this research intends to persuade commentators and the CJEU about the possible invalidity of this piece of secondary law, emulating the process that judges typically follow makes the arguments clearer, more relevant, and easier to follow. Therefore, the violations of fundamental rights will be reviewed using the proportionality scheme adopted by the Court in its existing jurisprudence on privacy, data protection, and security.

Second, the substantive arguments used to criticize the EU PNR are based not only on previous academic and parliamentary discussions but also on this jurisprudence. For reasons of space and time, it was only possible to select two main cases. Yet, the two cases were selected precisely because, in terms of the Court's substantive reasoning, they are crucial to assess the validity of PNR. The two cases selected are the Court's decision⁸ invalidating Directive 2006/24/EC on the retention of online and telecommunications data,⁹ and its Opinion¹⁰ on the EU-Canada PNR Agreement of 2014.¹¹

Directive 2006/24/EC tabled a system of blanket collection, retention, and processing of personal data on a massive scale for investigative purposes. Although it was a different system from PNR, it included many of the same features. Several aspects criticized by the Court in relation to Directive 2006/24/EC can therefore be criticized in relation to the intra-EU PNR using similar inferences and rationale.

Opinion 1/15 is about a PNR external agreement. So far, it is the only case decided by the Court on PNR and violations of fundamental rights. It is a detailed Opinion that could not be overlooked in research on this topic.

The structure of the doctrinal claim on fundamental rights follows the proportionality analysis used by the CJEU in these cases. Yet, not every problem for the rights of air passengers is discussed. While the Court criticized many aspects of Directive 2006/24/EC and the PNR Agreement without extensively elaborating its reasoning, the rigor of academic work relies on the strength and logic of its arguments. As such, this analysis focuses exclusively on three key problems. These are issues that recurrently surface in the literature, institutional debates, and jurisprudence for the gravity of their impact upon fundamental rights. They are the quantity and quality of collected data, the data retention period, and access rights by third parties.

The idea is that the depth of the study of these problems will suffice to demonstrate how the intra-EU PNR is disproportionate and, therefore, susceptible to being invalidated. Other problems could have been selected. However, only these allowed for a robust and thorough analysis based on a composite approach integrating different sources.

⁸ Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014 (ECLI:EU:C:2014:238).

⁹ 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 (OJ L 105, 13.4.2006).

¹⁰ Opinion 1/15, delivered on 26 July 2017 (ECLI:EU:C:2017:592).

¹¹ Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record (12657/5/13 REV 5, 23.6.2014).

3. Limitations

This work has certain limitations. The first regards its scope and the choice of issues under discussion. Concerns of time and space, together with the importance of fundamental rights and competence creep, have not allowed for an exploration of other topics.

Fundamental rights are a key matter explored in the literature. They could not, and should not, be avoided, especially because the flaws of the PNR Directive are mainly concerned with violations of privacy, data protection, and data rights.

The matter of conferral, or competence, however, is more original. No scholars have yet considered PNR and shared competences on security together. The discussions on creeping competences are often detached from solid analysis of concrete policies. This is particularly odd in the AFSJ, where the balance between the powers conferred to the EU and the original statehood powers that remain with the member states should be well-defined. There is a tension in the law permitted by ambiguous treaty law provisions, a tension which PNR embodies in a particular way.

A second limitation is that this research is concerned only with the intra-EU PNR scheme currently in force. It talks about related policies, the external agreements with third countries, and the 2011 proposal. Yet, they are not discussed in depth, being included to the extent they are relevant for understanding the Union's composite system. Otherwise, there would be no space to have a careful analysis of the current legislation.

This is a thesis on EU law. It does not include comparative studies, or field work, on national systems, for instance. The project could include comparisons with other policies and legislation, either internal or from abroad. PNR can, indeed, be studied from different angles and it raises many questions. But, it was necessary to be selective. The most pressing matter, at the moment, is to look at the recently approved system and find out whether it is characterized by major problems — and it is. There is already significant work on the agreements, national PNR schemes, and even the previous versions of the EU PNR. There was a gap, however, regarding Directive (EU) 2016/681.

Another limitation stems from the time of writing. This investigation began with the approval of this legislation, in 2016, lived through its transposition phase, until 2018, and finished after the Commission issued its first review, in 2020. While it has been an opportune and important moment to write about the EU PNR, this timing has also presented certain challenges. On the one side, there is more freedom to unpack possible problems that may have been flying under the radar. Still, it also means there are fewer authors with whom to enter into

dialogue about these problems. On the other, it might be rather too soon to see whether, and how, the functioning of the system actually encroaches upon fundamental rights and member states' agendas on security.

There are already pending cases before the Court claiming that the PNR Directive is disproportionate and invalid. The purpose of this research was, in a way, to prepare the ground for the judges, and its added value may change with a decision from Luxembourg. However, this work was written before there was even an opinion issued by an Advocate General (AG). Such added value will also remain due to the ample doctrinal analysis presented in this thesis and the originality of the research.

4. Structure of the study

This project is divided into three chapters, plus an introduction and concluding remarks. It goes from a broad contextualization and explanation of PNR in the EU to two thematic segments focusing on conferral and fundamental rights.

Chapter 1 explains what PNR is and how it works, providing basic terminology and a general introduction to its context and related policies. It then maps its evolution in three moments. The first moment addresses the legislation applicable to air bookings and explains the system that preceded PNR, called Advance Passenger Information (API). The second gives an account of the international agreements into which the Union has entered with third countries to exchange PNR data. It also looks at ongoing negotiations and the Commission's plans to adopt a multilateral legal tool. The final moment traces the development of a PNR scheme in the internal market, from the initial dialogues and failed draft to the approval, transposition, and review of Directive (EU) 2016/681.

Chapter 2 is the first thematic chapter. It argues that the Union went beyond its security competences, as the Directive goes past its constitutional bases and unduly encroaches upon national security. In fact, it unveils a tension in EU primary law provisions between the Union's conferred powers and national security exceptions which apparently give member states some discretion to define their policy agendas.

Its first section critically assesses the treaty law bases mentioned in the Directive, showing how they fail to justify a fully-fledged PNR. The legislation has provisions that do not find a sufficiently clear connection with those legal bases. The Union legislator also failed to find support in Article 16 of the Treaty on the Functioning of the EU (TFEU), which aims to protect individual personal data. The second section builds upon this to contend that the Union was not

competent to enact the intra-EU PNR system as it did. It explores the responsibilities of member states on national security in treaty law, until the Treaty of Lisbon. It then argues that, beyond its insufficient legal basis, PNR should be regarded as invalid because the issues falling under it should have been partially regulated by member states' legislators, mainly in light of the national security exception that can be found in Article 4(2) of the Treaty on EU (TEU), *in fine*.

Chapter 3 is the second thematic chapter and is divided into three autonomous, yet interdependent, parts. This classic topic in security studies is a cornerstone of research about PNR. Its first part reviews the literature on PNR and fundamental rights. It also appraises the legislative debates at the EP and comments on the input of member states, as well as supervisory and advisory bodies. The second looks at the jurisprudence of the CJEU. It lays out the formal structure that will be used to assess the Directive. This part distills the Court's decision regarding Directive 2006/24/EC and its Opinion on the EU-Canada 2014 Agreement. It unpacks the jurisprudential reasoning, and identifies major criticisms put forward by the Court regarding privacy, data protection, and the data right to individual notification. This is a step-by-step approach that clarifies the case law, starting with the identification of interferences with fundamental rights, and ending with proportionality assessments.

The formal structure and substantive inferences of these two parts are then brought together in the final part of this chapter. The purpose is to scrutinize the PNR Directive in detail. As such, the arguments used by the literature, MEPs, member states, advisory bodies, and, above all, the CJEU are combined to criticize it, in a manner similar to what the Court would do following a reference for a preliminary ruling regarding the validity of PNR.

The key conclusions of both thematic chapters are reiterated in the end. In summary, this project raises awareness about critical issues that affect a recent and far-reaching piece of legislation enacted by the EU. It provides an important contribution to studies on PNR, but also on security, law enforcement, the AFSJ, fundamental rights, conferral, and treaty law. It strives to be a step towards more sophisticated discussions on PNR, as well as towards rethinking the intra-EU system and the Union's security rationale. The concluding remarks also include some thoughts on the broader lessons that can be distilled from PNR, and its process of approval, for the Union and EU law.

Chapter 1.

An aviation story

“For example, it has been often criticized by security practitioners and critical activists alike, that it is not the lack of citizens’ data, but, reversely, the abundance of such data which poses a problem. It seems, at least in some cases, that public authorities store far more data than they can usefully process.”¹²

Introduction

On 27 April 2016, the Union enacted a Directive on PNR. It was approved together with a data protection package that changed Europe’s legal regime,¹³ headed by the GDPR. Yet, they are markedly different, not the least in their approach to fundamental rights. There is also a blunt contrast between the buzz that has surrounded the GDPR and the silence about PNR.¹⁴

This chapter tells the story of PNR. Following a contextual introduction, it explains what it is, what it does, and locates its place in the security agenda of the Union. The following sections detail its evolution in EU law, from the agreements with third countries to the intra-EU system. By explaining this security policy and providing a robust contextual approach, this chapter prepares the ground for the following analyses. Such a broad and updated study was missing from the scholarly writing on this topic.

With the growing number of security hazards, there are more and more systems being developed to process personal data for security purposes. This is happening outside but also within the Union. This work does not broadly tackle EU security policies. Instead, it focuses on PNR, which deserves the spotlight.

To tell a comprehensive story of PNR in the Union fills a gap in PNR studies, but also has the added value of shedding light on the difficulties the EU has faced in relation to this matter. PNR is diffusing globally. However, it can present serious problems to the constitutional and

¹² Kolliarakis, 2017: 234.

¹³ 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 (OJ L 119, 4.5.2016) and a draft proposal of what would later be Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) 45/2001 and Decision 1247/2002/EC (OJ L 295, 21.11.2018).

¹⁴ Bug & Bukow, 2017: 297 and 303.

legal systems of many countries, since PNR is an aggressive policy of criminal justice that relies on serious interferences with the privacy of individuals.

The external influence of the EU on third countries¹⁵ may help consolidate the spread of PNR, and the problems it brings. In fact, the issues arising in EU law will likely have relevance and resonance in other legal systems. This chapter is the first step in this journey, but it also helps to bear out the claims that will be made in this thesis as the issues explored further in the following chapters come into focus in the very story of PNR in Europe.

1. Check-in

1.1 A broader context

In June 1999, the European Council met in Cologne to reflect upon chief issues¹⁶ following the entry into force of the Treaty of Amsterdam.¹⁷ One of those issues was codifying the fundamental rights protected by the Union in a Charter.¹⁸ This would happen the following year. On 7 December 2000, in Nice, at another meeting of the European Council, the EP, the Council, and the Commission proclaimed the CFREU.

For the first time, the Union acquired a specific legal text incorporating political, civil, social, and economic rights that were already enshrined in other sources, either national, regional, or international.¹⁹ In 2009, with Lisbon, this document gained binding force and the same legal value as the TEU and the TFEU.²⁰

The CFREU shows the Union's commitment to guaranteeing fundamental rights. It is its "bill of rights."²¹ Yet, it protects rights whose scopes often collide. This happens, for example, with the rights to privacy, data protection, and security. While individuals have the right to see their private life²² and personal data²³ respected, they likewise have the right to be secure.²⁴ To ensure citizens are safe, the EU has repeatedly curtailed their privacy and intruded upon the

¹⁵ Wessel & Blockmans, 2012: 2.

¹⁶ Presidency conclusions of the European Council meeting in Cologne (3-4.6.1999), paragraph 1.

¹⁷ Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts (OJ C 340, 10.11.1997).

¹⁸ Presidency conclusions of the European Council meeting in Cologne (3-4.6.1999), paragraph 44.

¹⁹ Presidency conclusions of the European Council meeting in Nice (7-10.12.2000), paragraph 2.

²⁰ Hartley, 2014: 156.

²¹ Leczykiewicz, 2019: 131. See also Maduro, 2003: 277.

²² Article 7 CFREU.

²³ Article 8 CFREU.

²⁴ Article 6 CFREU.

protected status of their personal data, especially by approving secondary law to counter serious transnational crime and terrorism, under the ambitions and demands of its AFSJ.²⁵

These laws and policies are the result of negotiation and compromise, of political and legal choices that unveil the balance and tension between fundamental rights. Many were approved in the aftermath of concrete events. For instance, the terrorist events in the early 2000s, like those in New York, London, and Madrid, were followed by various reactions at EU level, with the legislator testing the limits of criminal law and the relationship between the constitutional and legal systems of the member states and the Union.

The result, however, is seldom optimal. While many security policies tend to devote some attention to privacy and data protection, these rights usually end up crowded out by security concerns. Besides, there are often insufficient assessments of their outcome, efficacy, and proportionality. For Valsamis Mitsilegas, the AFSJ has, thus, become a “patchwork of measures adopted swiftly, without detailed justification or impact assessment and resembling at times kneejerk reactions or quick fixes to complex issues, while presenting significant challenges to fundamental rights and the rule of law in Europe.”²⁶

Many such policies aim at anticipating and preventing further criminal and terrorist acts from taking place on EU soil. This has been designated by scholars as preventive, or pre-emptive, justice,²⁷ i.e., the use of state force to deter potential actions that may pose a danger to security.²⁸ Modern preventive justice relies extensively on profiling operations based on permanently updated risk criteria drawn from pools of big data. These data are normally collected by private actors, who are then required to convey them to law enforcement agencies. Pre-emptive justice techniques raise many questions, and form a heated topic in scholarly writing. They will not be addressed in detail for now. It suffices to say that, despite such questions, more and more laws are being approved, at EU and national level, which are shaped as preventive security tools.

The Schengen information system,²⁹ the rules to facilitate access and use of financial and bank account data,³⁰ or the agreement between the EU and the United States of America (US)

²⁵ A relatively innovative tool introduced by the Treaty of Amsterdam (Walker, 2006: 3).

²⁶ Mitsilegas, 2017: 5.

²⁷ De Goede, 2012: 57 ff., also calls it speculative security.

²⁸ Mitsilegas, 2017: 6.

²⁹ Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018).

³⁰ Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA (OJ L 186, 11.7.2019).

on the processing and transfer of financial messaging data³¹ are recent examples of such policies. They are based on the retention and processing of troves of personal data and, although expressing concerns about the privacy and data protection rights of individuals, end up encroaching upon these rights in favour of tighter security.

This is a growing trend in the AFSJ. All sorts of information can be collected, from biometric to financial, health, and travel data. PNR is in line with this legislative fashion. It is one of the most recent technologies applied to travel data, aiming at the prevention, detection, and countering of cross-border crime and terrorism through the retention and processing of personal information by law enforcement authorities. The data are extracted from bookings and reservations made by prospective air passengers who are, for the most part, unaware of the uses that will be made of their information.

PNR, however, is not the first Union policy to allow national and European agencies, private and public, to gather travel data. Air travel has been a sphere for testing in the implementation of new technologies, and the enforcement of legislation that allows police units to monitor EU citizens and third-country nationals.

1.2 Booking and ticketing

The first electronic ticketing systems appeared in the 1980s.³² The largest Global Distribution System was created in 1987 by a consortium between Air France, Iberia, Scandinavian Airlines System, and Lufthansa. It is called Amadeus and includes 95% of all booked airline seats worldwide,³³ making it the leading transaction processor in civil aviation. In 2016, it processed circa 595 million bookings and boarded 1382 million passengers. It includes air services but also other travel options, like rail and ferry.

Additional systems have appeared since then and, in 1989, the Council of the European Communities drafted a code of conduct for reservation technologies.³⁴ The aim was to

³¹ Council Decision of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program (OJ L 195, 27.7.2010).

³² Enerstvedt, 2017: 270.

³³ Amadeus, 2018.

³⁴ Council Regulation (EEC) 2299/89 of 24 July 1989 on a code of conduct for computerized reservation systems (OJ L 220, 29.7.1989), last amended by Council Regulation (EC) 323/99 of 29 October 1993 (OJ L 40, 13.2.1999). See also Commission Regulation (EEC) 2672/88 of 26 July 1988 on the application of Article 85 (3) of the Treaty to certain categories of agreements between undertakings relating to computer reservation systems for air transport services (OJ L 239, 30.8.1988), no longer in force, Commission Report on the application of Council Regulation (EEC) 2299/89 of 24 July 1989 (COM(97) 246 final, 9.7.1997), Recommendation 1/98 of the Article 29 Working Party, adopted on 28 April 1998, on airline Computerised Reservation Systems (CRS) (XV D/5009/98 final, WP

harmonize the purchase and use of Computerized Reservation Systems (CRS)³⁵ for scheduled air passenger services, and it especially targeted vendors and distributors. This code, repealed by Regulation (EC) 80/2009,³⁶ kept competition fair and protected consumers.³⁷ The Council not only sought to prevent anti-competitive behavior and guarantee that customers had access to impartial data,³⁸ but also to protect flyers regarding the processing of information undertaken by CRSs.³⁹

Although this Regulation introduced data protection norms, its underlying rationale is purely commercial. There is no indication that data can be used for non-commercial purposes. It states that processing, access, and storage serve only booking and the supply of tickets in transportation services.⁴⁰ The idea is that information collected by CRSs should only be used to fulfill the requirements of the contract.⁴¹ The drive for the code of conduct and the Regulation is far from law enforcement.

10), and Working document, adopted on 14 September 2001, on IATA Recommended Practice 1774 ‘Protection for privacy and transborder data flows of personal data used in international air transport of passengers and of cargo’ (5032/01/EN/Final, WP 49).

³⁵ According to Article 2(b) of Council Regulation (EEC) 2299/89, these are informatics structures “containing information about, inter alia, [participating] air carriers’ schedules, availability, fares, and related services.” This classification applies regardless the possibility of making reservations, or issuing tickets, and accessibility facilities to subscribers (e.g., travel agencies) or consumers. Similar information is mentioned by European Commission, 2021, where it reads that CRSs “act as technical intermediaries between the airlines and the travel agents [providing] their subscribers with instantaneous information about the availability of air transport services and the fares for such services.”

³⁶ Regulation (EC) 80/2009 of the European Parliament and of the Council of 14 January 2009 on a Code of conduct for computerised reservation systems and repealing Council Regulation (EEC) 2299/89 (OJ L 35, 4.2.2009).

³⁷ Paragraphs 1.6, 1.8, 3.6.1, and 3.6.4 to 3.6.6 of Opinion of the European Economic and Social Committee [EESC] on the Proposal for a regulation of the European Parliament and of the Council on a Code of conduct for computerised reservation systems (COM(2007) 709 final — 2007/0243 (COD)) (2008/C 224/12) (OJ C 224, 30.8.2008) already addressed PNR and privacy concerns. The Committee stated, for instance, that a “new regulation should be introduced whereby all PNRs created by CRS subscribers must be protected by the Codes Data Privacy articles without exception, including airlines who outsource the hosting of their PNR databases to CRS providers, as well as travel agencies, tour operators, corporations and any other source of booking connected to the CRS” (paragraph 3.6.6).

³⁸ Recital 4 of Regulation (EC) 80/2009.

³⁹ Recital 21 of Regulation (EC) 80/2009.

⁴⁰ Article 11 of Regulation (EC) 80/2009.

⁴¹ Article 11(2) of Regulation (EC) 80/2009. This could lead to some tension between this legislation and the PNR Directive. The former’s Article 11(1) refers to “[p]ersonal data collected in the course of the activities of a CRS.” It does not specify who collects them. Naturally, it is system vendors, air carriers, and other lawfully-interested parties, like travel agencies (subscribers), who do this. This means that data processing is, under this legislation, protected from uses that are incompatible with commercial operations, like security purposes. In Directive (EU) 2016/681, however, carriers are expected to transfer that same data to member states for processing (Article 6(1)) for “the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime” (Article 1(2)). It seems the protection provided in 2009 has been tacitly overridden in 2016, with respect to carriers. Only other entities remain unaffected, like system vendors who have to store identifiable bookings offline “within seventy-two hours of the completion of the last element in the individual booking and [destroy them] within three years [with access] allowed only for billing-dispute reasons” (Article 11(4) of Regulation (EC) 80/2009).

1.3 Transferring basic personal data

The first policy based on having air carriers hand passenger data to the police appeared in 2004. Council Directive 2004/82/EC⁴² instructs member states⁴³ to oblige airlines to transfer data whenever this is requested by border authorities.⁴⁴ These data are called API and consist of five items related to the itinerary and four concerning the passenger, namely their travel document information, nationality, names, and date of birth.

This legislation aims to monitor frontiers and to combat unlawful migration.⁴⁵ The purposes and scope of data processing operations under this policy differ significantly from those developed in 2016 under the PNR Directive. The data are stored, for instance, only temporarily.⁴⁶ They can be retained only up to 24 hours after the person crosses EU borders (i.e., after transmission takes place), unless they are needed for statutory functions and, even then, only in accordance with the conditions set out in the GDPR.⁴⁷ Member states must take appropriate action to compel carriers to erase any personal information they have obtained within 24 hours after arrival.⁴⁸ Furthermore, API systems require the collection of nine items of data. PNR requires the collection of 19.

Already in 2003, the Commission tabled the bases for future EU action on PNR, while clarifying the differences between API and PNR.⁴⁹ The Commission stressed that API strictly concerns the biometric data present in the machine-readable areas of passports and other identification documents. Plus, only in-bound flights are to be monitored and the use of such information is to be exceptional.⁵⁰ On the contrary, PNR makes the use of data the rule rather than the exception.

⁴² Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (OJ L 261, 6.8.2004).

⁴³ This follows the guidelines specified in Opinion 9/2006 of the Article 29 Working Party, adopted on 27 September 2006, on the implementation of Directive 2004/82/EC of the Council on the obligation of carriers to communicate advance passenger data (1613/06/EN, WP 127).

⁴⁴ This was a Spanish initiative in the aftermath of the 2004 terrorist attacks in Madrid and, according to its recital (13), builds upon Schengen.

⁴⁵ Articles 1 and 6(1) of Council Directive 2004/82/EC.

⁴⁶ Article 6(1), 1st paragraph, of Council Directive 2004/82/EC.

⁴⁷ Article 6(1), 2nd paragraph, of Council Directive 2004/82/EC.

⁴⁸ Article 6(1), 3rd paragraph, of Council Directive 2004/82/EC.

⁴⁹ Communication from the Commission to the Council and the Parliament on the transfer of air Passenger Name Record (PNR) data: A global EU approach (COM(2003) 826 final, 16.12.2003). This would be later developed by Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries (COM(2010) 492 final, 21.9.2010).

⁵⁰ Communication (COM(2010) 492 final, 21.9.2010), 3.

API is an identity authentication tool, while PNR serves criminal intelligence.⁵¹ PNR schemes make risk assessments to target and identify unknown persons, i.e., individuals who may be of concern to police agents but have been previously unidentified. It tries to link personal elements with serious crimes, as well as to compare data entries in order to identify connections and associations between potential suspects.⁵² PNR does not regulate movements at EU borders but, instead, co-exists with rules on entry and exit.⁵³

2. Working definitions

PNR has been used for more than 50 years by border authorities worldwide.⁵⁴ Collecting data from passengers by carriers is an obligation foreseen in the Convention on Civil Aviation,⁵⁵ also known as the Chicago Convention.⁵⁶ Data are used to identify and trace natural persons,⁵⁷ ranging from physical and observable traces, like age, gender, or height, to other types of information, such as names, addresses, or bank details.⁵⁸ The purposes of processing them are widening as they can provide important details that would, otherwise, be difficult to find.

PNR refers, in particular, to personal data collected in the context of transportation. It consists of unverified information transmitted in bulk and provided by prospective passengers during reservation and check-in. These records are examples of big data.

This project looks only at air carriage, so PNR here means the data of air travelers. They are collected by carriers and non-carrier economic operators, being stored in receipts⁵⁹ which can

⁵¹ Communication (COM(2010) 492 final, 21.9.2010), 4.

⁵² *Ibidem*.

⁵³ Commission staff working paper 'Impact Assessment' (SEC(2011) 132 final, 2.2.2011), 13.

⁵⁴ It first appeared in 1964, when International Business Machines and North-American airlines developed an electronic mechanism that would replace manual reservation and the repartition of fares (Han, et al., 2017: 1048 and 1049).

⁵⁵ Lord, 2019: 261.

⁵⁶ Convention on International Civil Aviation (adopted 7 December 1944, entered into force 4 April 1947) 15 UNTS 295 (7300/9).

⁵⁷ Which means that data to be collected in PNR schemes fall under the scope EU data protection laws, namely Article 4, 1st paragraph, of Regulation (EU) 2016/679, previously Article 2 of 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 (OJ L 281, 23.11.1995). Until the former's approval, carriers collected and processed PNR under this Directive and the external agreements. See also Article 2(a) of the Convention of the Council of Europe for the protection of individuals with regard to automatic processing of personal data (European Treaty Series 108, 28.1.1981).

⁵⁸ Their broad scope may present serious concerns regarding the guarantees aiming at protecting data. Some carriers, for instance, can store them for up to 40 years, according to Commission staff working paper (SEC(2011) 132 final, 2.2.2011), 34.

⁵⁹ They are usually not entirely filled as they are limited to what is provided in the reservation process. This means that certain slots are usually left empty, like baggage and billing details, or frequent flyer data. The model of these receipts has been standardized by the International Air Transport Association (IATA), which helps carriers, governments, and interested parties in designing and implementing PNR systems, according to Opinion on the

be saved in different databases, from departure control systems to frequent flyer programs. With the approval of the PNR Directive, that data must then be transferred to PIUs,⁶⁰ who are law enforcement entities specifically designated for processing and storing such information.⁶¹ PIUs can be created anew, or designated from existing bodies, but must be authorities which, under member state law, are competent to prevent, detect, investigate, and prosecute terrorist offenses and serious crime. They can later provide the collected data to other competent authorities, whenever requested, for further examination or other action.⁶²

The Council of Europe (CoE) recognized the need to regulate the use of personal data by law enforcement as early as 1987,⁶³ facing its growing use.⁶⁴ Such use originally targeted only certain flights, and processing was manual.⁶⁵ Data were handled exclusively by the police, or judicial authorities. However, nowadays, this has become a common security practice based on sophisticated automatic transfers.⁶⁶ This trend was accentuated in the aftermath of the 9/11 events and following debates on the need to effectively fight and prevent terrorism and serious crime of a transnational nature. It also shows that security is increasingly the result of cooperation between public and private actors.

data protection implications of the processing of Passenger Name Records of the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (T-PD(2016)18rev, 19.8.2016), 3. On this matter, see also Opinion 10/2004 of the Article 29 Working Party, adopted on 25 November 2004, on more harmonised information provisions (11987/04/EN, WP 100), namely its examples of notices in the Appendixes.

⁶⁰ PNR can be sent directly to the PIUs or, instead, to the EU Agency for the operational management of large-scale IT systems in the AFSJ. According to Article 16(4), 2nd paragraph, of Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011 (OJ L 295, 21.11.2018), member states may request its assistance as “a technical support tool to facilitate connectivity with air carriers...In such a case the Agency shall centrally collect the data from air carriers and transmit those data to the Member States via the common component or router.”

⁶¹ Articles 4 ff. of Directive (EU) 2016/681.

⁶² Article 7(1) of Directive (EU) 2016/681.

⁶³ Especially to balance the “interests of society in the prevention and suppression of criminal offences and the maintenance of public order...and the interests of the individual and his right to privacy,” according to the preamble of Recommendation of the Committee of Ministers to member states regulating the use of personal data in the police sector (R(87) 15, 17.9.1987). It comes after an update to Convention 108, following a 2011 public consultation promoted by the Bureau of the Consultative Committee, and Recommendation of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (CM/Rec(2010) 13, 23.11.2010).

⁶⁴ Due to the “explosion in the number of computers, an increase in their computing power, a reduction in their cost, and their increased availability in the home, within enterprises and within public administrations.” Legislation in the 1970s suddenly became inadequate to the capacity to collect, process, and share data of the new decentralized computer systems. Using such equipment with telecommunications permitted a quick availability of “telematic services which gradually began to pose their own problems,” in the words of the Study ‘New technologies: a challenge to privacy protection?’ prepared by the Committee of experts on data protection under the authority of the European Committee on Legal Co-operation (1989).

⁶⁵ Communication (COM(2010) 492 final, 21.9.2010), 4.

⁶⁶ *Ibidem*.

3. Flying abroad

PNR suits civil aviation, not the least as carriers gather data systematically.⁶⁷ While some member states had been using it, or were planning to implement it, for quite some time,⁶⁸ it first appeared in EU law through external agreements with third countries.

The first agreement was struck with the US. This was followed by accords with Canada and Australia. All of them have been reviewed by various actors, often more than once. In 2010, the Commission tabled a common global approach to PNR agreements, and there are ongoing negotiations with other third countries.

3.1 United States of America

The 9/11 terrorist events transformed many countries' political attitudes on security. The US quickly started reforming its surveillance apparatus on air transportation.⁶⁹ Since then, and under section 122.49b of the Code of Federal Regulations, together with the Aviation and

⁶⁷ European Commission, 2011: 5.

⁶⁸ According to Enerstvedt, 2017: 271, the United Kingdom has a PNR scheme since 2004. In 2011, it was the only member state with a fully-functioning system in place, while Belgium, Denmark, France, Spain, and Sweden were developing, or testing, their own programs (European Parliamentary Research Service, 2015: 7). This was made possible mostly through the funding of 14 national programs under Council Decision of 12 February 2007 establishing for the period 2007 to 2013, as part of General Programme on security and safeguarding liberties, the Specific Programme 'Prevention of and fight against crime' (2007/125/JHA) (OJ L 58, 24.2.2007).

⁶⁹ A first PNR scheme was introduced immediately in November 2001. It became a concern to the EU in terms of guaranteeing the security of its citizens' data, expressed in European Parliament Resolution of 13 March 2003 on transfer of personal data by airlines in the case of transatlantic flights (P5_TA(2003)0097) (OJ C 61 E, 10.3.2004). It says that the terrorist attacks led the US to a "root-and-branch overhaul of its legislation with a view to tightening internal security" (recital A), namely through the approval of Aviation and Transportation Security Act, Pub. L. 107-71, 115 Stat. 597 (2001) and Enhanced Border Security and Visa Entry Reform Act (EBSV), Pub. L. 107-73, 116 Stat. 543 (2002). The main problem was that the US Administration started requiring carriers to supply only the Passenger Manifest Information (a document with cabin and crew basic identification elements) but, subsequently, began to demand, "under threat of severe penalties, direct access to computerised reservation systems and, in particular, to [PNR], which [could] be linked up not only with identification data but with other information of the most various kinds...including sensitive information as defined in Article 8 Directive 95/46/EC" (recital B). The EP reproached the Commission's actions regarding data protection norms — as "reservation system databases may become de facto 'data-mining' territory for the US Administration" (recital C) under these changes — and the protection of airlines, "which [were] caught between a rock (if they follow[ed] Community law, they [were] liable to US sanctions) and a hard place (if they [gave] in to the US authorities' demands, they [fell] foul of the data protection authorities)" (2nd paragraph). See also European Parliament Resolution of 9 October 2003 on transfer of personal data by airlines in the case of transatlantic flights: state of negotiations with the USA (P5_TA(2003)0429) (OJ C 81 E, 31.3.2004), where the EP stressed its dissatisfaction with some issues regarding data protection safeguards presented by the US throughout the negotiations for a bilateral agreement, and Opinion 6/2002 of the Article 29 Working Party, adopted on 24 October 2002, on transmission of Passenger Manifest Information and other data from Airlines to the United States (11647/02/EN, WP 66). Some of the commentaries found in the latter, such as those on the necessity and justification of PNR transfers, would later be stressed in Working document of the Article 29 Working Party, adopted on 25 November 2005, on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (2093/05/E, WP 114), 13 and 14.

Transportation Security Act and Article 44909(c)(3) of the US Code, air companies operating flights that depart, land, or fly over US territory with a foreign origin or destination must transfer their passengers' PNR to the Customs and Border Protection of the Department of Homeland Security (DHS). The data are collected from the reservation systems of carriers and transferred before departure. They are then processed by DHS agents to determine which passengers need to be subject to additional inspection and control measures, or detained in the course of criminal investigations.

European air companies had to comply with these measures under threat of losing landing rights, or accepting heavy economic sanctions. Even though compliance with this obligation violated data protection norms present in Directive 95/46/EC,⁷⁰ most airlines chose to break EU law rather than to suffer direct economic disadvantages. They were “caught between a rock and a hard place,”⁷¹ until the negotiations between the Commission and the US led the former to desist from law enforcement actions against carriers that complied with American standards while it assessed the adequacy of US data protection norms. On the other hand, American authorities decided not to enforce their PNR legislation until 5 March 2003.

In the first customs talks between the EU and the US, it was agreed that the parties would strive for a mutually acceptable⁷² bilateral agreement, under the conditions of Article 25(6) of Directive 95/46/EC. Even so, the Commission insisted on a multilateral agreement under the umbrella of the International Civil Aviation Organization (ICAO).⁷³

In 2003, the Commission emphasized that the relationship with the US should be based on a balanced and tenable compromise.⁷⁴ It had to aim at the prevention of terrorism and transnational crime, respect privacy and other fundamental rights, demand a reasonable cost from carriers, and be convenient and secure for travelers. The Commission wanted an adequacy decision⁷⁵ supplemented by a “«light» bilateral international agreement”⁷⁶ and mechanisms to

⁷⁰ Not least because the US did not present an adequate level of protection while processing such data, as required by its Article 25. In this regard, the US Transport Security Administration conducted tests in 2004 and 2005 which revealed its contractors did not collect, process, or store data according to the Privacy Act, Pub. L. 93-579, 88 Stat. 1896 (1974).

⁷¹ An expression used by a representative of Lufthansa in an interview promoted by europarl.eu to Timothy Kirkhope, MEP and *rapporteur* of the EP's Committee on Civil Liberties, Justice and Home Affairs responsible for drafting the PNR Directive, to illustrate the difficult position of airlines at the time.

⁷² Joint Statement 'European Commission/US customs talks on PNR transmission' (2003), paragraph 7.

⁷³ *Idem*, paragraph 8.

⁷⁴ Communication (COM(2003) 826 final, 16.12.2003), 4.

⁷⁵ Assisted by Opinion 4/2003 of the Article 29 Working Party, adopted on 13 June 2003, on the level of protection ensured in the US for the transfer of passengers' data (11070/03/EN, WP 78).

⁷⁶ Communication (COM(2003) 826 final, 16.12.2003), 4.

inform passengers in a comprehensive, precise, and timely manner. Plus, it insisted on the use of the push method⁷⁷ regarding data transfers.⁷⁸

The EU and the US signed a first PNR Agreement in 2004.⁷⁹ It was a short text referring to legislation and documents stemming from the discussions between the contracting parties. The terms and limits of data transfers, for instance, were not included, as they were defined in the Undertakings issued by the DHS.⁸⁰ They would serve as the basis for an adequacy decision subsequently issued by the Commission.⁸¹ Only in the following agreements would a specific provision be introduced to certify that the DHS presented sufficient data protection guarantees.

The Agreement ensured that carriers located in the Union, operating flights to and from the US, would process PNR present in their CRSs as defined by the DHS. The DHS would access their databases through the pull method until new technology enabled the adoption of the push method. Data were to be treated without negative discrimination and in compliance with US statutory and constitutional standards.⁸²

Though it was reviewed in September 2005,⁸³ the CJEU invalidated⁸⁴ the Commission's adequacy decision of 14 May 2004 and the Council's decision of 17 May 2004 to conclude the

⁷⁷ The pull method consists in law enforcement having direct access to carriers' databases to withdraw information. The push method, on the contrary, obliges law enforcement agents to ask airlines for data, who then transmit the records. The latter, however, does not mean the transmission of data is fully left at the discretion of air carriers. Unlawful noncompliance may result in severe penalties and there are legal criteria compelling carriers to transfer the information. In the case of the EU-US agreements, for example, the transfer decision rests upon the DHS, according to US law, and regardless the method used.

⁷⁸ Communication (COM(2003) 826 final, 16.12.2003), 5 and 8.

⁷⁹ Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection attached to the Council Decision of 17 May 2004 (2004/496/EC) (OJ L 183, 20.5.2004).

⁸⁰ Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection, United States Federal Register, volume 69, number 131, 41543 ff.

⁸¹ Commission Decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection (2004/535/EC) (OJ L 235, 6.7.2004). It followed the critical European Parliament Resolution of 31 March 2004 on the draft Commission decision noting the adequate level of protection provided for personal data contained in the Passenger Name Records (PNRs) transferred to the US Bureau of Customs and Border Protection (2004/2011(INI)) (P5_TA(2004)0245) (OJ C 103 E, 29.4.2004). Both documents were informed by Opinion 2/2004 of the Article 29 Working Party, adopted on 29 January 2004, on the adequate protection of personal data contained in the PNR of air passengers to be transferred to the United States' Bureau of Customs and Border Protection (US CBP) (10019/04/EN, WP 87).

⁸² Agreement (OJ L 183, 20.5.2004), paragraph 4.

⁸³ Commission staff working paper (SEC(2011) 132 final, 2.2.2011), 5.

⁸⁴ The Article 29 Working Party had already alerted the Commission that it had only partially respected its previous opinions when it enacted that adequacy decision and that the EP could summon the CJEU to review it, as well as the Agreement, for potential violations of fundamental rights. This can be found in Opinion 6/2004, adopted on 22 June 2004, on the implementation of the Commission decision of 14-V-2004 on the adequate protection of personal data contained in the Passenger Name Records of air passengers transferred to the United States' Bureau of Customs and Border Protection, and of the Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (11221/04/EN, WP 95), 2. It issued a second opinion a few months later, namely Opinion 8/2004, adopted on 30 September 2004, on the information for passengers

Agreement.⁸⁵ As such, the 2004 Agreement was replaced by a provisional text in 2006.⁸⁶ It expired on 31 July 2007 and was substituted by a follow-up Agreement⁸⁷ with a structure and content similar to its predecessors.⁸⁸ Moreover, 1 January 2008 was set as the deadline to change transfer procedures from the pull to the push method for all carriers who managed to implement the necessary technical means.

This Agreement was accompanied by a letter⁸⁹ from Michael Chertoff, Secretary of Homeland Security, to Luís Amado, President of the Council, explaining how the DHS handled and stored PNR. It did not expressly revoke the 2004 Undertakings but it gave a detailed account of the functioning of the system and American standards.

concerning the transfer of PNR data on flights between the European Union and the United States of America (11733/04/EN, WP 97).

⁸⁵ See joined cases C-317/04, *European Parliament v Council of the European Union*, and C-318/04, *European Parliament v Commission of the European Communities*, 30 May 2006 (ECLI:EU:C:2006:346), paragraphs 67 to 69. The Article 29 Working Party quickly issued Opinion 5/2006, adopted on 14 June 2006, on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States (1015/06/EN, WP 122) stressing the importance that a new deal be drafted as soon as possible to “avoid a legal gap...for the transfer of passenger data and to ensure that the rights and freedoms of passengers continue to be protected” (2). An emergency backup was developed a few months later, in Opinion 7/2006, adopted on 27 September 2006, on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States and the urgent need for a new agreement (1612/06/EN, WP 124).

⁸⁶ Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security attached to the Council Decision of 16 October 2006 (2006/729/CFSP/JHA) (OJ L 298, 27.10.2006). As usual, it came after an analysis from the EP, namely European Parliament Recommendation to the Council of 7 September 2006 on the negotiations for an agreement with the United States of America on the use of passenger name records (PNR) data to prevent and combat terrorism and transnational crime, including organised crime (2006/2193(INI)) (P6_TA(2006)0354) (OJ C 305 E, 14.12.2006). The EP was not as critical as it had been in Resolution (OJ C 103 E, 29.4.2004). Still, it insisted on certain aspects that had been mentioned two years earlier and that it deemed not to have been satisfactorily addressed, such as the need to extend the protection of personal data that was enjoyed by US passengers to EU citizens, or the appeal for caution on the establishment of an indirect EU PNR scheme on US soil due to the considerable amount of processed data that could be transferred from US authorities to law enforcement units operating in the member states outside proper criminal investigations and judicial cooperation schemes. See also Opinion 2/2007 of the Article 29 Working Party, adopted on 15 February 2007, on information to passengers about transfer of PNR data to US authorities (XXXX/07/EN, WP132).

⁸⁷ Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement) attached to the Council Decision of 23 July 2007 (2007/551/CFSP/JHA) (OJ L 204, 4.8.2007). This Agreement was informed by European Parliament Resolutions of 14 February 2007 on SWIFT, the PNR agreement and the transatlantic dialogue on these issues (P6_TA(2007)0039) (OJ C 287 E, 29.11.2007) and of 12 July 2007 on the PNR agreement with the United States of America (P6_TA(2007)0347) (OJ C 175E, 10.7.2008). It was also reviewed by the Article 29 Working Party, which published Opinion 5/2007, adopted on 17 August 2007, on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007 (01646/07/EN, WP 138).

⁸⁸ Both the US and the Australian agreements tend to be provisional, as was noted on Communication from the Commission to the European Parliament and the Council ‘Overview of information management in the area of freedom, security and justice’ (COM(2010) 385 final, 20.7.2010), 17.

⁸⁹ Letter to the Council Presidency and the Commission from the Department of Homeland Security (DHS) of the United States of America, concerning the interpretation of certain provisions of the undertakings issued by DHS on 11 May 2004 in connection with the transfer by air carriers of passenger name record (PNR) data (OJ C 259, 27.10.2006).

The agreements have been subject to different reviews.⁹⁰ The 2007 Agreement was reviewed in 2010 by the Commission with the input and assistance of authorities from the member states and the US,⁹¹ following an informal meeting at Toledo which culminated in a joint declaration on aviation security.⁹² This renegotiation was also due to the entry into force of the amendments of the Treaty of Lisbon.

A new Agreement was put forward in 2012, acknowledging previous arrangements, joint reviews, and even input from the European Data Protection Supervisor (EDPS).⁹³ This was more extensive, comprising 27 provisions. A reciprocity clause was added, but specified only that the Agreement should be modified to guarantee complete reciprocity⁹⁴ if an EU PNR system were to be implemented in the meanwhile. As before, this was a provisional text providing for periodic joint reviews⁹⁵ and which should expire seven years after its entry into force,⁹⁶ if the parties did not renew it.⁹⁷

The results of the latest joint review were published in 2017. It took place in July 2015, in Washington, D.C., following recommendations from 2013, which were implemented, or are in the course of being implemented. One of the more telling changes concerned fully applying the push method to data transfers,⁹⁸ with the DHS assisting air carriers on a technical level. Redress mechanisms were also modified for transparency reasons.

Despite the EU finding that the DHS was broadly compliant with the Agreement, it still issued some recommendations. The number of accesses to PNR data without a nexus with the US increased between 2013 and 2015 with no obvious cause. The Commission suggested this fact should be documented and form the basis for further study. It also stressed the need to

⁹⁰ Despite their provisional nature, only the Canadian and Australian agreements have sunset clauses (Commission (COM(2010) 385 final, 20.7.2010), 24).

⁹¹ And after European Parliament Resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada (P7_TA(2010)0144) (OJ C 81E, 15.3.2011).

⁹² US Department of Homeland Security, 2010. In the section on information sharing, the parties stated that they should find ways to improve cooperation amidst all agents involved in aviation based on previous agreements and joint reviews.

⁹³ Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security attached to the Council Decision of 26 April 2012 (OJ L 215, 11.8.2012). See also Opinion of the EDPS on the proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security (OJ C 35, 9.2.2012).

⁹⁴ Article 20 of Agreement (OJ L 215, 11.8.2012).

⁹⁵ Article 23 of Agreement (OJ L 215, 11.8.2012).

⁹⁶ Article 26(1) of Agreement (OJ L 215, 11.8.2012).

⁹⁷ Article 26(2) of Agreement (OJ L 215, 11.8.2012).

⁹⁸ Report from the Commission to the European Parliament and the Council on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security {SWD(2017) 14 final} {SWD(2017) 20 final} (COM(2017) 29 final, 19.1.2017), 3.

restrict and control the number of agents with access rights. The codes to access sensitive data, mechanisms to anonymize data, and response times for dealing with passenger requests were also targeted and recommended for review. Finally, the Commission suggested that more details should be publicly provided to passengers by the DHS regarding the processing of data.

3.2 Canada

On 7 March 2005, the Council of the EU authorized the Commission to negotiate an agreement with Canada on the transfer and processing of API and PNR data.⁹⁹ This came in the aftermath of legislation empowering the Canada Border Services Agency (CBSA) to collect data from passengers flying to its territory from international destinations. It was a similar case to the hardening of security regulations by the US after 9/11.

Nonetheless, the obligation to feed authorities with PNR data was phased in by the CSBA¹⁰⁰ from March 2003 to September 2004. Economic sanctions for noncompliance were tabled only in February 2005 and the EU benefited from an extended derogation until July. This allowed authorities to reach an understanding regarding possible international agreements. In any case, there seemed to be a sense of urgency from the EU in drafting the proposal.¹⁰¹ The Commission even said it represented the easiest, fastest, and most effective way to provide a legally adequate resolution.¹⁰²

The main concern was, again, that privacy and data protection safeguards were lower in Canadian than in European legislation. Hence, the Commission started working on a proposal, based on a 2003 Communication¹⁰³ and the expertise drawn from negotiations with the US.

⁹⁹ Following Opinion 1/2005 of the Article 29 Working Party, adopted on 19 January 2005, on the level of protection ensured in Canada for the transmission of Passenger Name Record and Advance Passenger Information from airlines (1112/05/EN, WP 103) and Opinion of the European Data Protection Supervisor, adopted on 15 June 2005, on the proposal for a Council Decision on the conclusion of an agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information (API) / Passenger Name Record (PNR) data (OJ C 218, 6.9.2005).

¹⁰⁰ Explanatory memorandum of the Proposal for a Council Decision on the conclusion of an Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information (API)/Passenger Name Record (PNR) data (COM(2005) 200 final, 2005/0095 (CNS), 19.05.2005), 2.

¹⁰¹ This had also happened with the first EU-US Agreement. The Council sent two letters to the EP, dated 25 March and 28 April 2004, stressing the urgency to produce an opinion as “the fight against terrorism, which justifies the proposed measures, is a key priority of the European Union. Air carriers and passengers are at present in a situation of uncertainty which urgently needs to be remedied. In addition, it is essential to protect the financial interests of the parties concerned,” according to Opinion of AG Philippe Léger, delivered on 22 November 2005 (ECLI:EU:C:2005:710), paragraphs 8 and 11. Curiously, the EP rejected both requests.

¹⁰² On such basis, the Commission argued it complied with the principle of proportionality (Explanatory memorandum of Proposal (COM(2005) 200 final, 2005/0095 (CNS), 19.05.2005), 3 and 4).

¹⁰³ Communication (COM(2003) 826 final, 16.12.2003).

Canada committed to strengthening data protection norms, and the draft was based on previous adequacy decisions.¹⁰⁴

The Council of the EU approved the outline attached to the Commission's proposal, despite a negative opinion from the EP.¹⁰⁵ It recognized that the negotiations had struck a reasonable compromise between freedom and security,¹⁰⁶ from a procedural standpoint. The guarantees and binding clauses, however, did not appear sufficiently explicit in the text.¹⁰⁷ As such, it did not sanction the negotiations and instructed the Council to wait until the CJEU had delivered a decision in joined cases C-317/04 and C-318/04.

The Agreement entered into force on 22 March 2006,¹⁰⁸ notwithstanding the efforts of the EP. Its Article 8 and Annex III opened the floor for joint reviews on its implementation to take place on an annual basis, or as agreed between the parties.¹⁰⁹

It was, indeed, jointly reviewed in November 2008 and the CBSA was found to apply its commitments to a substantial degree.¹¹⁰ Although the supporting adequacy decision expired in September 2009, Canadian authorities maintained high data protection standards until a new agreement was negotiated. A renegotiation would be tabled in 2010, under request of the EP,¹¹¹ following the entry into force of the Treaty of Lisbon.

¹⁰⁴ Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (2002/2/EC) (OJ L 2, 4.1.2002) based on that Canadian regulation (SC 2000, c. 5). See also Opinion 2/2001 of the Article 29 Working Party, adopted on 26 January 2001, on the adequacy of the Canadian Personal Information and Electronic Documents Act (5109/00/EN, WP 39). That adequacy decision would later be replaced by Commission Decision of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency (2006/253/EC) (OJ L 91, 29.3.2006), based on section 107.1 of Customs Act, RSC 1985, c. 1 (2nd Supp.), Access to Information Act, RSC 1985, c. A-1, Privacy Act, RSC 1985, c. P-21, and paragraph 148(d) of Immigration and Refugee Protection Act, SC 2001, c. 27. As before, the Article 29 Working Party was consulted and issued Opinion 3/2004, adopted on 11 February 2004, on the level of protection ensured in Canada for the transmission of Passenger Name Records and Advanced Passenger Information from airlines (10037/04/EN, WP 88).

¹⁰⁵ European Parliament Legislative Resolution of 7 July 2005 on the proposal for a Council decision on the conclusion of an Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information (API)/Passenger Name Record (PNR) data (COM(2005)0200 – C6-0184/2005 – 2005/0095(CNS)) (P6_TA(2005)0294) (OJ C 157E, 6.7.2006).

¹⁰⁶ *Idem*, recital (A), first item.

¹⁰⁷ *Idem*, recital (A), second item.

¹⁰⁸ Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data (OJ L 82, 21.3.2006).

¹⁰⁹ Unlike the EU-US Agreement, this one foresaw a Joint Committee to accompany the implementation of procedures and address any issues, or disputes, that might arise afterwards (Article 6).

¹¹⁰ Explanatory memorandum of the Recommendation for a Council Decision authorising the opening of negotiations on an Agreement between the European Union and Canada for the transfer and use of Passenger Name Record (PNR) data to prevent and combat terrorism and other serious transnational crime (COM(2017) 605 final, 18.10.2017).

¹¹¹ European Parliament Resolution (OJ C 81E, 15.3.2011).

The Commission forwarded a recommendation to the Council allowing for these renegotiations in September. The EP authorized them¹¹² and, in December, the Council agreed to undertake them. They only took place, nevertheless, in May 2013.¹¹³

The new text was signed in June 2014, with an expected duration of seven years.¹¹⁴ It was submitted for the approval of the Council and the EP. On 25 November 2014, the latter requested¹¹⁵ an Opinion from the CJEU to inquire about the text's compatibility with the treaties and the CFREU. On 26 July 2017,¹¹⁶ the Court issued its first decision on the conformity of an international agreement with the CFREU.¹¹⁷ The Agreement was found to be incompatible with EU primary law. It directly conflicted with Articles 7, 8, 21, and 52(1) CFREU.

Just like a legislator outlining and revising a legal document,¹¹⁸ the Court listed the adjustments it thought necessary to make the Agreement lawful. Passengers should be clearly informed about which data were to be transferred to Canada, for instance. Plus, the use of data by the CBSA should be strictly limited, subject to a prior review by judicial or other independent bodies, and only serve to fight terrorism and serious international crime. The Court also deemed it inappropriate that PNR could be further transferred to other third countries without an adequacy decision from the Commission.¹¹⁹

After this decision, the CBSA expressed its will to renegotiate the Agreement, and the Commission recommended that the Council issue a decision to reopen negotiations.¹²⁰ The idea was to modify the text according to the instructions of the CJEU.¹²¹ Discussions between the EU and Canada were concluded at the beginning of 2019. Until the writing of this text, Canada

¹¹² European Parliament Resolution of 11 November 2010 on the global approach to transfers of passenger name record (PNR) data to third countries, and on the recommendations from the Commission to the Council to authorise the opening of negotiations between the European Union and Australia, Canada and the US under the EU external strategy on Passenger Name Record (PNR) (P7_TA(2010)0397) (OJ C 74E, 13.3.2012).

¹¹³ According to Proposal for a Council Decision on the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data 2013/0251 (NLE) (COM(2013) 529 final, 18.7.2013). This proposal would later be sent to the EDPS, which would issue an Opinion on the proposals for Council decisions on the conclusion and the signature of the agreement between Canada and the European Union on the transfer and processing of passenger name record data (OJ C 51, 22.2.2014).

¹¹⁴ Article 28(1) of Agreement (12657/5/13 REV 5, 23.6.2014). Its number 2 foresaw its automatic renewal for a subsequent term of seven years, unless otherwise decided by the parties.

¹¹⁵ European Parliament Resolution of 25 November 2014 on seeking an opinion from the Court of Justice on the compatibility with the Treaties of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data (2014/2966(RSP)) (P8_TA(2014)0058) (OJ C 289, 9.8.2016).

¹¹⁶ Following Opinion of AG Paolo Mengozzi, delivered on 8 September 2016 (ECLI:EU:C:2016:656).

¹¹⁷ Kuner, 2018: 858.

¹¹⁸ Vidaschi & Graziani, 2018.

¹¹⁹ Opinion 1/15, paragraph 232.

¹²⁰ Based on Article 218 TFEU.

¹²¹ This was highlighted also in Annex 1 to Recommendation (COM(2017) 605 final, 18.10.2017), which contained the directives for the renegotiation. Another key point was to include "all the safeguards required in order for it to be compatible with Articles 7, 8, 21 and 52 (1)" CFREU.

was reviewing the legal aspects of the new draft, which should ensure the confidentiality and security of data.¹²²

3.3 Australia

Before concluding an agreement with the EU, Australia already required providers of international air services to transmit the PNR they collected to the Australian Customs and Border Protection Service.¹²³ The Council authorized the Presidency and the Commission to begin negotiations in February 2008.¹²⁴ After a meeting that approved a general approach, a provisional Agreement was signed on 30 June.¹²⁵ It was binding to all member states, except those who had first to adapt their legal regimes.¹²⁶

The Agreement was somewhat different from those struck with the US and Canada. It came with a long Annex in which the parties developed important aspects, such as rules on disclosure and data protection. It included a clause about joint reviews,¹²⁷ though the parties were free to determine most of their details. The first review was supposed to take place after four years,¹²⁸ unless an intra-EU PNR system was approved.

¹²² Canada-EU Summit joint declaration of 17 and 18 July 2019, paragraph 11.

¹²³ This obligation was based on section 64AF of the Customs Act 1901 (Cth), Crimes Act 1914 (Cth), Migration Act 1958 (Cth), Freedom of Information Act 1982 (Cth), Customs Administration Act 1985 (Cth), and Privacy Act 1988 (Cth).

¹²⁴ The EP, nonetheless, makes reference to a first round of negotiations between the Union and Australia already in 2003 and 2004 in Recommendation of 22 October 2008 to the Council concerning the conclusion of the Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian customs service (2008/2187(INI)) (P6_TA(2008)0512) (OJ C 15 E, 21.1.2010). This was a critical text, starting with the fact the EP lamented not having been informed of those negotiations under the principle of loyal cooperation. It stressed that it should always be consulted in matters affecting citizens' fundamental rights, regardless the lack of will from other institutions. This document also mentions that, in 2003, the Australian government requested an investigation from the Commission into whether it complied with adequacy levels for PNR transfers. In response, the Commission asked for an advisory opinion and the Article 29 Working Party produced Opinion 1/2004, adopted on 16 January 2004, on the level of protection ensured in Australia for the transmission of Passenger Name Record data from airlines (10031/03/EN, WP 85).

¹²⁵ Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian customs service attached to the Council Decision 2008/651/CFSP/JHA of 30 June 2008 (OJ L 213, 8.8.2008).

¹²⁶ These were Belgium, the Czech Republic, Finland, Germany, Hungary, Ireland, Latvia, Malta, the Netherlands, and Poland, according to item "I/A" of Note from the Presidency to the Coreper/Council (10439/08, 10.6.2008). Austria added a statement to the minutes (Annex I) arguing that Article 12, on data retention, should be read as allowing the transfer and retention of data only under the purpose limitation set in Article 5(1) and not of PNR data as a united group, so as to comply with the principle of proportionality. Moreover, Germany and Malta asked to have written statements (Annex II) confirming their need to adapt the Agreement to their constitutional frameworks, in order to respect their legal and constitutional bases.

¹²⁷ Article 9 of Agreement (OJ L 213, 8.8.2008).

¹²⁸ The EP reproached the Agreement for not setting a fixed deadline for the first review. It thus called on the Commission and Council to require a joint review no later than June 2010 in Recommendation (OJ C 15 E, 21.1.2010).

This provisional Agreement was replaced by a definitive one¹²⁹ that entered into force on 1 June 2012.¹³⁰ It was to be jointly reviewed after one year¹³¹ and remain in force for the following seven years.¹³² This first review took place in Canberra, in August 2013. It focused on certain aspects of the implementation, namely the masking of data and onward transfers to third countries. It was similar to what was foreseen in the agreements with the US and Canada, being based on replies to a questionnaire sent by the Commission.

An EU team then visited Australia's Passenger Analysis Unit and the parties met to discuss implementation. It seemed its border services were respecting all terms and conditions, and that they were constantly working to improve the automatic detection and erasure of sensitive information. In fact, PNR receipts were analyzed against risk factors in a targeted manner, which reassured the EU of the restricted access to passenger data.¹³³

3.4 Prospective agreements and a revised global approach

PNR is spreading across the world. Japan, New Zealand, Saudi Arabia, Singapore, South Africa, and South Korea, for instance, are implementing, or testing PNR systems. Though some are willing,¹³⁴ they have not settled agreements with the Union.¹³⁵

Mexico has had legislation instructing carriers to provide customs and border agencies with data from international flights since 2012. Still, its PNR system has not been implemented, in practice, and authorities have been prevented from applying sanctions to European airlines for not supplying them with such information. In 2015, Mexico pressed the Union to start negotiations. Following the proposal of Dimitris Avramopoulos, Commissioner for Migration,

¹²⁹ This new Agreement was additionally based on Auditor-General Act 1997 (Cth), Ombudsman Act 1976 (Cth), and Public Service Act 1999 (Cth).

¹³⁰ Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service (OJ L 186, 14.7.2012). This was preceded by a Proposal for a Council Decision on the conclusion of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service (2011/0126 (NLE)) (COM(2011) 281 final, 19.5.2011), which had been assessed by the EDPS in its Opinion on the proposal for a Council decision on the conclusion of an Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service (OJ C 322, 5.11.2011).

¹³¹ Article 24(2) of Agreement (OJ L 186, 14.7.2012).

¹³² Article 26(1) of Agreement (OJ L 186, 14.7.2012).

¹³³ Report from the Commission to the European Parliament and the Council on the joint review of the implementation of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service {SWD(2014) 236 final} (COM(2014) 458 final, 10.7.2014), 2.

¹³⁴ South Korea is, at least since 2008, in negotiations with the Union, according to European Parliament Recommendation (OJ C 15 E, 21.1.2010).

¹³⁵ Communication (COM(2010) 492 final, 21.9.2010), 2 to 4.

Home Affairs and Citizenship, in June,¹³⁶ the Council mandated the Commission to enter into negotiations, as Mexico is a relevant partner in Latin America. Negotiations began immediately in July,¹³⁷ but they are currently stalled.

Since 2014, Argentina has also adopted legislation to collect PNR. The Spanish delegation to the Council of the EU raised this issue in March 2015, pressing the Union to initiate conversations with Mexico and Argentina as soon as possible, especially in light of the implications that delays in striking international agreements with these third countries could have for the commercial interests of carriers.¹³⁸ Nevertheless, there have been no developments regarding forthcoming agreements.

More recently, the Council of the EU authorized the Commission to begin talks with Japan to draft an international PNR agreement.¹³⁹ It was stressed, in a press release, that the text would respect fundamental rights by applying all required mechanisms foreseen in EU law.¹⁴⁰

The existing bilateral agreements have considerable differences. They have been outlined separately, on a case-by-case basis, an approach which has resulted in disparities in how data are managed.¹⁴¹ The Commission has considered renegotiating them and creating a model for future ones.¹⁴² This idea was already present in a Communication from 2003, in which the

¹³⁶ The Article 29 Working Party had sent a letter to Avramopoulos, on PNR obligations Mexico, dated 6 February 2015, expressing concern about potential transfers to Mexican authorities. Representatives from carriers had, apparently, talked with the Working Party, complaining about its risks. The Working Party pointed out the lack of legal base in EU law, as well as of an adequacy decision, or similar instrument, assuring the proper processing of citizens' data. It thus called on the Commission to promote solutions that would prevent airlines from breaking EU and Mexican law, stressing that this was applicable to any third country which failed to enforce appropriate measures to protect PNR data from incoming EU flights.

¹³⁷ At the time, there were 17 main European air companies flying regularly to Mexico, including Air France-KLM Royal, British Airways, and Iberia, according to Joint statement: Beginning of negotiations between Mexico and the European Union on PNR data transmission (STATEMENT/15/5374, 14.7.2015).

¹³⁸ Note from the Spanish delegation to the Council on the information by the Commission on the PNR legislation adopted by Mexico and the Republic of Argentina requesting the transfer of PNR data from the EU (6857/15, 5.3.2015).

¹³⁹ Article 1(1) of Council Decision authorising the opening of negotiations with Japan for an agreement between the European Union and Japan on the transfer and use of Passenger Name Record (PNR) data to prevent and combat terrorism and serious transnational crime (5378/20, 4.2.2020).

¹⁴⁰ Council of the European Union, 2020.

¹⁴¹ Communication (COM(2010) 492 final, 21.9.2010), 5. See also, in general, Jones, 2012.

¹⁴² It claimed, in Communication (COM(2003) 826 final, 16.12.2003), 9 and 10, that a multilateral framework under ICAO should replace the agreements as PNR data transfers are a global matter, not a bilateral issue. This position was subsequently reinforced in Communication (COM(2010) 492 final, 21.9.2010), 11, where it concluded that the "EU should explore the possibility of replacing, in the medium term, bilateral agreements by a multilateral agreement between all countries that use PNR data." In fact, the use of PNR was discussed for the first time in ICAO at the 12th session of its Facilitation Division, which took place from 22 March to 1 April 2004. It committed itself to the creation of guidelines that should be used by operators worldwide to prevent the unilateral, or bilateral, request for PNR transfers, especially due to the technical, legal, and even financial constraints that could ensue for carriers. These guidelines were developed and presented on different occasions, until their latest revised version was released to the public in 2010, in a document called Guidelines on Passenger Name Record (PNR) data (9944, 2010). An important aspect affecting the uniformity of data transfers is the format of messaging. Machine-readable travel document programmes, API, and PNR featured as item 7 on the agenda of the high-level

Commission said it wanted to achieve uniformity in the EU's external actions on PNR through a set of broad criteria that could be used to guide future dialogues with third countries.¹⁴³

The review of the global approach to transnational PNR transfers was being completed when the Commission published a Communication giving a comprehensive account of how data were managed in the AFSJ. It fostered the idea that citizens are entitled to know who processes and handles their personal information, and for what reasons.¹⁴⁴ As such, the Commission listed all EU law applicable to systems based on data processing for law enforcement or immigration purposes. It also laid out common principles that should be observed in the development and assessment of tools for managing data.

The Commission issued a second Communication, in September 2010, reaffirming the will to standardize external policies, and the aim of implementing those principles.¹⁴⁵ It justified revisiting its global approach on PNR for five main reasons.¹⁴⁶ The first was that the EU has a duty to cooperate with third countries in fighting terrorism. An effective way of doing so is by exchanging relevant data with foreign authorities. A unified PNR transfer messaging system can only increase efficiency and closer cooperation. Secondly, it is easier to ensure data protection and control with standardized transfers, namely by having a single processing model.¹⁴⁷ In third place, the obligations for carriers must be clear and harmonized to lower the aviation industry's cost pressure and to maintain fairness in the area.¹⁴⁸ A clear and consistent legal basis for PNR data transfers is the only way to achieve this. Fourthly, differences in

conference on aviation security that took place in Montréal, from 12 to 14 September 2012, which recommended that ICAO should incorporate the PNRGOV message format developed by an IATA/Air Transport Association of America Passenger and "Airport Data Interchange Standards Reservations Sub-Group composed of experts from the airline industry and interested States." This was endorsed by IATA, ICAO, and the World Customs Organization. They also supported PAXLST, the standardized messaging format for API (paragraphs 3.1 ff. and 4.2 of High-level conference on aviation security working paper on Passenger Name Record (PNR) data and its role in aviation security (HLCAS-WP/5, 4/6/12)). See also Management summary on passenger-related information of the IATA, ICAO, and World Customs Organization ('Umbrella Document' version 2.0, July 2017).

¹⁴³ Communication (COM(2003) 826 final, 16.12.2003), 3.

¹⁴⁴ Communication (COM(2010) 385 final, 20.7.2010), 3.

¹⁴⁵ This was despite the EP suggesting the Commission should table "a single model and a draft mandate for negotiations with third countries...no later than mid-July 2010 [to establish a] coherent approach on the use of PNR [through a] single set of principles to serve as a basis for agreements with third countries," in Resolution (OJ C 81E, 15.3.2011), paragraph 7.

¹⁴⁶ Following Opinion of the EDPS on the Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries (OJ C 357, 30.12.2010) and Opinion 7/2010 of the Article 29 Working Party, adopted on 12 November 2010, on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries (622/10/EN, WP 178).

¹⁴⁷ The Commission noted that adherence by third countries to common criteria on data protection through the ratification of international legislation should be essential to allowing data transfers. It then identified the principles that requesting countries must respect in this matter, adding that previous adequacy decisions could be used as a guide for determining what is appropriate (Communication (COM(2010) 492 final, 21.9.2010), 8). Nonetheless, it is not clear whether and how the Commission wanted to add these criteria to formal adequacy decisions.

¹⁴⁸ Communication (COM(2010) 492 final, 21.9.2010), 6.

external agreements are inevitable, as countries have different legal orders. Yet, a common set of provisions is key to treating passengers equitably, which hangs on a common and uniform approach to data transfers. Finally, the Commission underlined that security checks at airports are getting longer and more meticulous. Adding to the data which need processing is likely to increase waiting times in transit. Simpler common electronic transfers taking place before passengers cross EU borders can make travelling quicker and law enforcement more targeted.¹⁴⁹

The Commission would reaffirm in 2017 the need for common criteria and robust legal safeguards to protect fundamental rights. It also suggested drafting a model agreement which could clarify the EU law obligations for third countries, in an effort towards data sharing options that are both legally acceptable and viable on the long term.¹⁵⁰

4. A long departure

Legislation for an intra-EU PNR underwent a long incubation period.¹⁵¹ Before 2016, only a few member states had specific legislation, or were trying to implement it.¹⁵²

On 9 October 2003, the Commission held a meeting with specialists to start preparing a common position on PNR.¹⁵³ The Council of the EU would call on it, in early 2004, to draft an instrument to use passenger data for border security and related concerns,¹⁵⁴ like the fight

¹⁴⁹ Communication (COM(2010) 492 final, 21.9.2010), 7.

¹⁵⁰ Communication from the Commission to the European Parliament and the Council ‘Exchanging and protecting personal data in a globalised world’ (COM(2017) 7 final, 10.1.2017), 15.

¹⁵¹ Opinion of the European Economic and Social Committee on the ‘Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime’ (COM(2011) 32 final — 2011/0023 (COD)) (2011/C 218/20) (OJ C 218, 23.7.2011), paragraph 3.4. See also McKeever, 2021: 15.

¹⁵² According to Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime {SEC(2011) 132 final} {SEC(2011) 133 final} (COM(2011) 32 final, 2011/0023 (COD), 2.2.2011), 4. The fear of not having harmonization, in Timothy Kirkhope’s words, was that, as several member states were beginning to consider “setting up PNR systems...national measures [might] diverge in several respects, including the purpose of the system, the period of data retention, the structure of the system, the geographic scope and the modes of transport covered. It [was] also very likely that once the complete regulatory framework on the use of PNR data in those Member States [was] adopted, there [would] be divergent rules on data protection and on the measures ensuring the security of data transfers. As a result, up to 27 considerably diverging systems could be created. That would result in uneven levels of protection of personal data across the EU, security gaps, increased costs and legal uncertainty for air carriers and passengers alike.”

¹⁵³ Communication (COM(2003) 826 final, 16.12.2003), 9.

¹⁵⁴ Note from the General Secretariat of the Council of the European Union ‘Declaration on combating terrorism’ (7906/04, 29.3.2004), 9.

against terrorism.¹⁵⁵ PNR was not expressly mentioned but debates on the security of air transportation were preparing the ground for its advent.¹⁵⁶

A year later, the Hague Programme to strengthen freedom, security, and justice in the Union was approved. The Council recalled that the Commission had been asked to submit a plan for a uniform approach to using data from air passengers for the protection of borders and civil aviation.¹⁵⁷ Still, only the action plan to implement that Programme would explicitly mention PNR, as well as the follow-up Council meeting of 13 July 2005, which instructed the Commission to present a proposal on PNR by October.¹⁵⁸

One of the measures of the Programme on cooperation among police and judicial authorities was the sharing of PNR data.¹⁵⁹ Under this topic, the Council and Commission proposed to look at a common approach on passenger data, jointly review the PNR Agreement with the US, finish the negotiations with Canada and Australia, and define international guidelines that would ensure privacy when accessing PNR receipts.¹⁶⁰

4.1 Harmonizing the common space

The first proposal for a PNR Directive appeared in 2007¹⁶¹ but, as it was not adopted in due time, it became outdated with the entry into force of the Treaty of Lisbon. In 2010, the Council

¹⁵⁵ Defined in Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA) (OJ L 164, 22.6.2002).

¹⁵⁶ Objective 4 of Annex I ‘European Union strategic objectives to combat terrorism (Revised plan of action)’ to Note (7906/04, 29.3.2004), 16, provided for the protection and safety of international transportation and the efficient control of borders. See also the references to the need for technology to protect EU borders through the gathering and transferring of air passenger data and to enhance cooperation regarding “the protection of airports, seaports, and aircraft security arrangements in order to deter terrorist attacks and address the vulnerabilities in domestic and overseas transport operations,” in Note from the Presidency and CT Co-ordinator of the Council of the European Union to the Council/European Council on the European Union counter-terrorism strategy (14469/4/05 REV 4, 30.11.2005), 10.

¹⁵⁷ The Hague Programme: strengthening freedom, security and justice in the European Union (2005/C 53/01) (OJ C 53, 3.3.2005), 8.

¹⁵⁸ Declaration of the Extraordinary Council of the European Union condemning the terrorist attacks on London (11116/05 (Presse 187), C/05/187, 13.7.2005), point 6.

¹⁵⁹ Council and Commission Action plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union (2005/C 198/01) (OJ C 198, 12.8.2005), 10.

¹⁶⁰ *Idem*, 11.

¹⁶¹ Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes {SEC(2007) 1422} {SEC(2007) 1453} (COM(2007) 654 final, 2007/0237 (CNS), 6.11.2007), issued after European Parliament Resolution of 20 November 2008 on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes (P6_TA(2008)0561) (OJ C 16E, 22.1.2010). This proposal was accompanied by an impact assessment based on a questionnaire sent out in 2006 and whose results were discussed, in Brussels, on 2 February 2007. This questionnaire aimed to achieve a comprehensive overview of the different positions on PNR, and so it was sent to member states and their data protection authorities, as well as the EDPS, Association of European Airlines, Air Transport Association of America, European Regions Airline Association, International Air Carrier Association, and IATA. They committed to supporting security mechanisms in civil aviation through “industry-driven security initiatives such

of the EU called upon the Commission to propose new legislation, with particular care to guarantee an adequate level of data protection.¹⁶²

A second proposal appeared in February 2011.¹⁶³ It was one of more than 40 actions aimed at tackling the EU's most pressing challenges in the Commission's internal security strategy.¹⁶⁴ Despite some developments on privacy guarantees,¹⁶⁵ it was rejected, on 24 April 2013, by 30 votes to 25, at the EP's Committee on Civil Liberties, Justice and Home Affairs (LIBE). It was argued that the collection, processing, and retention of passenger data were not proportionate. Additionally, fundamental rights were inadequately protected.

On 30 August 2014, the European Council called on the EP and the Council to resume work on PNR.¹⁶⁶ It was not until 2015, however, in the aftermath of two terrorist attacks in Paris, that the debate gained momentum and substantial developments took place.¹⁶⁷ After the first attack, in January, the EP approved a Resolution in which it committed to work for the implementation

as...Passenger Name Record," according to paragraph 8 of Resolution on aviation security, adopted at the 73rd IATA annual general meeting (4 to 6 June 2017), mentioned in Commission staff working paper (SEC(2011) 132 final, 2.2.2011), 5. This proposal was extensively discussed in the councils on Justice and Home Affairs, even after being approved. Most provisions were accepted by consensus in the working groups, according to Note from the Presidency of the Council of the European Union to the Multidisciplinary group on organised crime (5618/2/09 REV 2, 29.6.2009), paragraphs 1 and 2. See also 2008 Opinion of the European Union Agency for Fundamental Rights [FRA] on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes.

¹⁶² The Stockholm Programme — An open and secure Europe serving and protecting citizens (2010/C 115/01) (OJ C 115, 4.5.2010), 19.

¹⁶³ It apparently took into consideration several recommendations from supervisory bodies, namely Opinion of the EDPS on the draft proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes (OJ C 110, 1.5.2008), Joint opinion of the Article 29 Data Protection Working Party (145, 5.12.2007) and the Working Party on Police and Justice (01/07, 18.12.2007) on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007 (02422/07/EN), and the 2008 Opinion of FRA.

¹⁶⁴ This was part of a broad-range course of action headed by Cecilia Malmström, Commissioner for Home Affairs, to change the way security concerns are tackled. From one issue at a time, in a "silo mentality," she believed in developing a common response that combined efforts and forced actors to work together. PNR, in particular, was brought in under the strategic objective of disrupting "international crime networks threatening our society" (European Commission, 2010).

¹⁶⁵ It was considered insufficiently limited to the strictly necessary, according to Opinion 10/2011 of the Article 29 Working Party, adopted on 5 April 2011, on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (00664/11/EN, WP 181). See also Opinion of the EDPS on the proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (2011/C 181/02) (OJ C 181, 22.6.2011) and FRA's Opinion 1/2011 on the Proposal for a Directive on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011) 32 final).

¹⁶⁶ In that same year, the Commission asked FRA to put forward some instructions on the processing of PNR for police purposes. The agency then published, on 26 February 2014, a list of Twelve operational fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data. These were clear and simple instructions "of «dos and don'ts» on how to operationalise fundamental rights when establishing national PNR systems" (1). Since then, FRA has included sections on PNR in its annual Fundamental Rights Report. The 2017 Report was particularly detailed, giving an account of several aspects of Directive (EU) 2016/681.

¹⁶⁷ Saulnier-Cassia, 2017: 209.

of an intra-EU system until the end of 2015. It advised the Commission to consider carefully the ramifications of the CJEU's decision regarding the data retention Directive, as well as its potential effects on the EU PNR. The EP also encouraged it to consult experts from various fields, namely the police and intelligence services, to bring in their viewpoints on the need and proportionality of such system.¹⁶⁸

At the meeting on the European Agenda on Security, the EP maintained the need to adopt a common PNR scheme, by the end of the year, with all the safeguards to respect fundamental rights.¹⁶⁹ It committed itself to assisting the Commission in working towards a proposal that would meet the criteria of necessity and proportionality.¹⁷⁰ It also underlined that future security schemes should contain reciprocity mechanisms.¹⁷¹ In November 2015, the EP would approve another Resolution, wherein it insisted on the importance of PNR, never ceasing to stress the need to protect fundamental rights.¹⁷²

Despite this apparent urgency, a PNR Directive would only be approved in April 2016, following other terrorist events, this time in Brussels.¹⁷³ This is a similar text to the one

¹⁶⁸ European Parliament Resolution of 11 February 2015 on anti-terrorism measures (2015/2530(RSP)) (P8_TA(2015)0032) (OJ C 310, 25.8.2016), paragraph 13. In the same passage, the EP asked the Council to work on the data protection package so that both legislations could be developed in parallel.

¹⁶⁹ In a letter to Claude Moraes, Chairman of the LIBE Committee of the European Parliament, on EU PNR, dated 19 March 2015 (Ref. Ares(2015)1241920), Isabelle Falque-Pierrotin, the Article 29 Working Party's Chairperson at the time, stated that the Working Party was pleased with some of the developments on data protection. Yet, the necessity of such a system was still insufficiently justified. The Letter alluded to recent rulings of the CJEU, stressing that the offenses and data retention period should be abbreviated and justified, and that a sunset clause should be added to ensure that the system's necessity was reviewed on a regular basis. These points were explored in an Appendix to the Letter, along with detailed guidelines for implementation. The EDPS would also publish Opinion 5/2015 'Second opinion on the proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime' (OJ C 392, 25.11.2015).

¹⁷⁰ On this note, the EDPS demonstrated support for the EU legislator on security matters. Yet, it considered that PNR should be reviewed. The initial words of its STATEMENT EDPS/2015/12 (10.12.2015), were that "Europe is under attack [and that, in] the wake of new terrorist atrocities, the EU and the governments of its Member States are under pressure to take meaningful action." Yet, although the "data protection community continues to offer its unconditional support in these difficult times [it will also help] the legislator in re-assessing the necessity and proportionality of any proposed measure, including EU PNR...in the context of current events and evidence [as] fighting crime and terrorism are clearly legitimate objectives, but any measure must respect the rule of law."

¹⁷¹ European Parliament Resolution of 9 July 2015 on the European Agenda on Security (2015/2697(RSP)) (P8_TA(2015)0269) (OJ C 265, 11.8.2017), paragraph 27.

¹⁷² European Parliament Resolution of 25 November 2015 on the prevention of radicalisation and recruitment of European citizens by terrorist organisations (2015/2063(INI)) (P8_TA(2015)0410) (OJ C 366, 27.10.2017), paragraph 42. The references to PNR came under the heading 'Stepping up the exchange of information on terrorist radicalisation in Europe.' Despite the apparent relevance of PNR, the EP considered that the Directive would "be just one measure in the fight against terrorism, and that a holistic, ambitious and comprehensive strategy on counterterrorism and the fight against organised crime, involving foreign policy, social policy, education policy, law enforcement and justice, [was] required to prevent the recruitment of European citizens by terrorist organisations."

¹⁷³ In Joint Statement by First Vice-President Timmermans and Commissioner Avramopoulos on the adoption of the EU Passenger Name Record (PNR) Directive by the European Parliament (STATEMENT/16/1404, 14.4.2016), the Commission made clear that PNR was a scaling step in the EU's response to terrorism and serious crime following the Paris and Brussels incidents. Some commentators even argue that the intra-EU PNR would

presented in 2011.¹⁷⁴ It was approved with 461 votes in favor, 179 against, and 9 abstentions, having entered into force on 24 May. The process was relatively quick,¹⁷⁵ although it followed the ordinary legislative procedure.¹⁷⁶ Following on from discussions at the Council on 18 November and 15 December 2015, a first reading and issuing of an opinion by the EP took place on 14 April 2016.¹⁷⁷ The text was accepted with some modifications, and was then subject to new discussions on 15 and 18 April. It was finally passed, at first reading, on 21 April, and signed by the presidents of the EP and Council simultaneously with the data protection package, on 27 April 2016.¹⁷⁸

4.2 Transposing the Directive

Two years after their approval, on 25 May 2018, the data protection package and the PNR Directive had to be transposed to the member states' internal legal orders. This was an odd moment in the history of data protection laws in the EU, as they have contrasting purposes and opposite effects upon the fundamental rights of European citizens. The Union managed to “both strengthen and weaken its privacy on the same day.”¹⁷⁹

On 21 February 2018, the Bulgarian presidency of the Council of the EU convened a conference on the future of PNR. Several political figures and representatives from 24 member states participated, as well as from Australia, the US, and Switzerland. Many EU agents were present too. The discussions were informed by the work undertaken by the Informal Working Group on PNR (IWG-PNR). They discussed the quality, exchange, protection, and proper use of data, alongside the difficulties regarding the implementation of the Directive, the

not have been finished if it were not for the succession of terrorist attacks in 2015 and 2016. See, for instance, Servent & MacKenzie, 2017: 402.

¹⁷⁴ Even some important documents accompanying the current Directive, like opinions from supervisory bodies or reports from member states, date back to 2011, or previous years. The legislative process is available at <https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:32016L0681> (accessed on 12 November 2018).

¹⁷⁵ Estelle Massé and Lucie Krahulcova, contributors to the human rights group Access Now, wrote in its blog that such approval was “no more than a knee-jerk reaction to the political climate after the terrorist attacks in Paris and Brussels.” They have also stressed that the reason why the awareness raised by advisory bodies as to the PNR’s proposals insufficiencies on human rights have “not served as a huge red flag for our lawmakers remains a mystery. We can only conclude that the current political climate is creating a distracting fog” (Massé & Krahulcova, 2016).

¹⁷⁶ As this is legislation aiming to regulate police cooperation, this secondary source had to be issued in the form of a Directive, according to Article 82 TFEU. See also Articles 87, 289, and 294 TFEU.

¹⁷⁷ Legislative Resolution of 14 April 2016 on the proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011)0032 – C7-0039/2011 – 2011/0023(COD)) (P8_TA(2016)0127) (OJ C 58, 15.2.2018).

¹⁷⁸ After this process, the EP issued Background note ‘EU Passenger Name Record (PNR) directive: an overview’ (20150123BKG12902) (1 June 2016) to provide an account of the context leading up to Directive (EU) 2016/681.

¹⁷⁹ Access Now, 2016.

relationships of member states with third countries, access rights by Europol, and best practices against terrorism and serious crime.¹⁸⁰

A few days later, on 26 February, the Council of the EU issued a note stating that the implementation of the Directive was being regularly discussed at the IWG-PNR and by the Commission.¹⁸¹ It commended the progress achieved, especially due to the exchange of lessons learned and the financial and legal assistance provided by the Commission through bilateral cooperation. The Council urged member states to reflect on whether all available mechanisms were being considered in the adoption of the Directive, identify the main outstanding difficulties, and share what they expected from other member states and EU institutions for a timely implementation.

Still, few member states managed to transpose it on time. Already in November 2016, the Commission published an implementation plan with six “indicative milestones”¹⁸² and a timeline. It acknowledged, however, that implementing PNR schemes compatible with the Directive requires a considerable amount of money, time, and technological expertise.¹⁸³ These milestones are mentioned in succeeding progress reports. The report of 7 June 2018¹⁸⁴ says that only 14 member states had communicated to the Commission the measures they had taken to

¹⁸⁰ Note from the Presidency of the Council of the European Union to the Working Party on Information Exchange and Data Protection (DAPIX) on the Conference on the future of PNR data - effective use and challenges (6104/18, 23.2.2018).

¹⁸¹ Note from the Presidency of the Council of the European Union to the Permanent Representatives Committee/Council on the Directive (EU) 2016/681 on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime - Implementation of the PNR Directive / Exchange of views (6017/18, 26.2.2018).

¹⁸² According to Commission staff working document ‘Implementation plan for Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime’ (SWD(2016) 426 final, 28.11.2016), these were: i) implement the Directive; ii) establish the PIUs; iii) develop the means to process PNR; iv) obtain human resources to work in the PIUs; v) set connections with competent authorities; and vi) engage with carriers and make PNR systems interoperable.

¹⁸³ This had already been recognized in Communication from the Commission to the European Parliament, the European Council and the Council ‘First progress report towards an effective and genuine security Union’ (COM(2016) 670 final, 12.10.2016), 6. The idea of implementing milestones comes originally from this document. It is also quite clear regarding the challenges in exchanging data to achieve such milestones, based on available technology. Despite funding and assistance programs, in 2016, only the United Kingdom had an operative PIU, with France and Hungary being the only member states that could have one by the end of that year. The Communication further revealed the incapacity of member states to process collected data, and indicated that 11 had not started transposing the Directive. The Commission thus asked for extra funding to the amount of 70 million Euros for the period 2017-2020 and decided to increment in 3.8 million Euros the value allocated to “facilitate the exchange of PNR data between Member States and the Europol.”

¹⁸⁴ Date of the first meeting between the member states and the Commission to go over the application of Directive (EU) 2016/681 after the deadline for transposition.

transpose the Directive,¹⁸⁵ though the online list of national transpositions counted 19 member states, at the time.¹⁸⁶

The report also states that critical obstacles, like the lack of technical capabilities, had been overcome in 24 member states. Despite this progress, an unsatisfactory level of implementation led the Commission to stress that it would keep helping member states, but that it would also resort to infringement actions if needed.¹⁸⁷ This warning showed the Commission's belief that PNR is essential for the Union's approach to serious crime and transnational terrorism,¹⁸⁸ even if it has issued no efficiency reports confirming this.

By 2020, 24 member states had indicated that they had transposed the Directive. As for the defaulting member states, the first review report says that "Slovenia ha[d] notified partial transposition and Spain, which ha[d] not notified any transposition measures, was referred to the Court of Justice on 2 July 2020 for failure to implement the Directive."¹⁸⁹

The common protocols and data formats foreseen in Article 16 of Directive (EU) 2016/681 were adopted in 2017.¹⁹⁰ The remaining implementation work was monitored by the IWG-PNR. By October 2018, it had met seven times.¹⁹¹ Australia presented its system in the last meeting, after Canada had done so in April. This has been useful mostly in assisting member states in learning how third countries are using PNR, as well as in tackling operational problems.¹⁹²

¹⁸⁵ These were Belgium, Croatia, Estonia, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Slovakia, and the United Kingdom.

¹⁸⁶ National transposition legislation and accompanying documents are publicly accessible at <https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32016L0681> (accessed on 9 October 2018). Denmark opted out of the Directive due to its 'blanket' opt-out position regarding the EU's Justice and Home Affairs. It has a national PNR system since 2006, although its implementation falls short in terms of legislative and political will, according to Lund, 2017.

¹⁸⁷ The report reveals the Commission sent, on 19 July 2018, "letters of formal notice to 14 Member States (Austria, Bulgaria, Cyprus, the Czech Republic, Estonia, Finland, France, Greece, Luxembourg, [t]he Netherlands, Portugal, Romania, Slovenia and Spain) for failing to communicate the adoption of national legislation which fully transposes the PNR Directive."

¹⁸⁸ Communication from the Commission to the European Parliament, the European Council and the Council 'Fifteenth progress report towards an effective and genuine security Union' (COM(2018) 470 final, 13.6.2018), 10 and 11.

¹⁸⁹ Report from the Commission to the European Parliament and the Council on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2020) 305 final, 24.7.2020), 5.

¹⁹⁰ See Commission Implementing Decision (EU) 2017/759 of 28 April 2017 on the common protocols and data formats to be used by air carriers when transferring PNR data to Passenger Information Units (OJ L 113, 29.4.2017).

¹⁹¹ Note from the General Secretariat of the Council to the Working Party on Information Exchange and Data Protection (DAPIX) on the update on the Informal Working Group on PNR^[1] 7th IWG PNR meeting (12825/18, 17.10.2018).

¹⁹² Note from the General Secretariat of the Council to the Working Party on Information Exchange and Data Protection (DAPIX) on the Update on the Informal Working Group on PNR (10139/18, 21.6.2018).

4.3 The 2020 review

The Commission should have conducted a review of the Directive, and then submitted an account of its findings to the EP and the Council, by 25 May 2020.¹⁹³ The legislator left the door open for a thorough review, as the Commission was given powers to make amendments by means of a legislative proposal.¹⁹⁴

The report was delayed two months, having been presented in July. Yet the review, together with its more detailed accompanying document,¹⁹⁵ did not match the apparent expectations of the legislator in 2016. They provided a general context of the Directive and listed key implementation aspects. The Commission considered that member states had implemented data protection standards while transposing it¹⁹⁶ and it found almost no elements needing review, from the processing of data to the retention period.

This first review served more to confirm the seeming need for an intra-EU PNR system than to appraise challenging aspects, even in light of recent case law of the CJEU.¹⁹⁷ Aspects that could be developed, like extending it to data collected by non-carrier economic operators or using PNR to address issues beyond terrorism and serious crime, were postponed because the Commission believed this should be preceded by a detailed impact assessment.¹⁹⁸ It concluded that, at that point, no adjustments could be suggested, since it was the moment for ensuring that the Directive was being properly applied.¹⁹⁹

¹⁹³ Article 19(1) of Directive (EU) 2016/681.

¹⁹⁴ Article 19(4) of Directive (EU) 2016/681.

¹⁹⁵ Commission staff working document accompanying the ‘Report from the Commission to the European Parliament and the Council on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime {COM(2020) 305 final} (SWD(2020) 128 final, 24.7.2020).

¹⁹⁶ Report (COM(2020) 305 final, 24.7.2020), 5.

¹⁹⁷ *Idem*, footnotes 15 and 16.

¹⁹⁸ Report (COM(2020) 305 final, 24.7.2020), 11.

¹⁹⁹ *Idem*, 12.

Chapter 2.

Creeping competences: A (not so) clear runway

“Lastly, there is the question of how to ensure that a redefined division of competence does not lead to a creeping expansion of the competence of the Union or to encroachment upon the exclusive areas of competence of the Member States and, where there is provision for this, regions. How are we to ensure at the same time that the European dynamic does not come to a halt? In the future as well the Union must continue to be able to react to fresh challenges and developments and must be able to explore new policy areas.”²⁰⁰

Introduction

The previous chapter has explained the context and development of PNR in Europe. Chapters 2 and 3 focus, instead, on particular legal issues that the intra-EU system gives rise to, with a view to demonstrating that the Directive should be regarded as invalid if it is challenged before the CJEU. This first thematic chapter presents a topic which tends to be absent from debates on security and law enforcement. It argues that the EP and the Council of the EU went beyond their conferred powers when adopting the PNR Directive. Not only did they exceed the limits laid down by the Directive’s legal bases, but certain features should have been left for the member states to regulate, as they still hold some responsibilities regarding the definition of their national security agendas.

Very few authors talk about conferral when writing on PNR. Neither is it a matter of regular discussion at an institutional level. Yet, debates on how the security-related powers of the member states are limited by the attribution of competences to the EU in the AFSJ are far from settled. This chapter tries to bridge PNR studies and the literature examining the AFSJ’s legal bases and the principle of conferral, in order to critically assess whether primary law offers sufficient support, in terms of competences, for the adoption of the Directive.

EU treaties have been gradually expanding Union competences on security, easing the construction of an AFSJ. However, the treaties also contain provisions which embody what the EP has called national security exceptions.²⁰¹ These exceptions restrict the scope of the Union’s competences. While the general rule is that the Union is free to legislate in areas of shared competences, these exceptions aim to prevent the EU from approving binding legal acts that are too intrusive on member states’ responsibilities in security.

²⁰⁰ Annex I ‘Laeken Declaration on the future of the European Union’ to the Presidency conclusions of the European Council meeting in Laeken (DOC/01/18, 14-15.12.2001), 5.

²⁰¹ European Parliament Resolution (OJ C 265, 11.8.2017), recital (C).

The problem, however, is that treaty law is not clear on the line separating the powers conferred upon the EU and the powers that remain with the member states. The Union has taken advantage of this ambiguity to approve various legal acts over the years that may be thought to bypass those exceptions. This has given rise to a tension in the law, between the TEU, the TFEU, EU secondary law, and member state security legislation. This tension has resurfaced with PNR, making this an ideal opportunity to rekindle the debate on the Union's creeping competences in the AFSJ.

This chapter is divided into two parts. The first critically reviews the legal bases used by the legislator to approve the Directive. It argues that the retention of PNR goes beyond what is allowed under Article 87(2)(a) TFEU and that the legislator should have enacted it using a multiple legal basis, including Article 16 TFEU as well, which is concerned with the protection of data. The second part stretches the argument considerably further and consolidates the claim that the Directive should be regarded as invalid. It starts by discussing the allocation of competences in the AFSJ and by exploring the concept of national security exceptions. It then analyzes Articles 72 TFEU and 4(2) TEU, *in fine*. These two provisions contain national security exceptions that could apply in relation to the example of PNR, and should have prevented the adoption of a fully-fledged system.

1. Reviewing the legal bases

An adequate legal basis is indispensable for the lawful exercise of EU competence,²⁰² as well as a prerequisite for the validity of EU legal acts. This principle is applicable to international agreements, as well as internal legislation. In fact, the CJEU has stated that:

The choice of the appropriate legal basis has constitutional significance. Since the Community has conferred powers only, it must tie the Protocol to a Treaty provision which empowers it to approve such a measure. To proceed on an incorrect legal basis is therefore liable to invalidate the act concluding the agreement and so vitiate the Community's consent to be bound by the agreement it has signed.²⁰³

The first part of this chapter critically reviews the legal bases of the Directive. On the one hand, it will be argued that the bases sustaining PNR do not allow for indiscriminate retention of personal data by law enforcement, contrary to what is foreseen by the PNR scheme. The

²⁰² Cremona, 2006: 6.

²⁰³ Opinion 2/00, delivered on 6 December 2001 (ECLI:EU:C:2001:664), paragraph 5.

claim is that the EU legislator adopted an act providing for retention of data beyond what is allowed in treaty law. On the other hand, it will also be argued that the Directive should have been based on an additional legal basis, which the Court has found to be essential regarding law enforcement systems that process and retain big data of a personal nature. This first part of the chapter is thus about an insufficient legal basis and about a missing legal basis. Still, it will be demonstrated that even the addition of this missing legal basis would not make the legal bases relied on sufficient as a matter of law.

1.1 Article 82(1)(d) TFEU

The Directive identifies its treaty law bases by claiming that the EP and the Council of the EU had regard to the TFEU, namely Articles 82(1)(d) and 87(2)(a).²⁰⁴ The former states that the EP and the Council may adopt measures to smooth collaboration between member states' police and judicial bodies in criminal cases and regarding the execution of court rulings. Article 87(2)(a) TFEU confers power on the EU to establish measures concerning the collection, storage, analysis, or exchange of relevant information, for establishing police cooperation involving all the member states' competent authorities.

In Opinion 1/15, the Court found that Article 82(1)(d) did not serve as legal basis for the Union to conclude the EU-Canada PNR Agreement.²⁰⁵ This followed the Opinion of AG Mengozzi, who admitted to having reservations about whether the proposed text could be found to specifically promote the purposes set out in that provision.²⁰⁶ The AG's main concern was that the Agreement encouraged judicial cooperation only in limited circumstances. Cooperation was, apparently, beyond its scope and seemed to be merely a secondary effect.

There was only one explicit reference to cooperation in the Agreement. Article 6 foresaw that Canada should share "relevant and appropriate analytical information containing PNR data obtained under this Agreement with Europol, Eurojust, within the scope of their respective mandates, or the police or a judicial authority of a Member State of the European Union."²⁰⁷ In Mengozzi's view, this meant that Canadian judicial authorities would be obliged to cooperate with the EU in exchanging data. Yet:

²⁰⁴ Opening remarks of Directive (EU) 2016/681.

²⁰⁵ According to the opening remarks of Proposal for a Council Decision (COM(2013) 529 final, 18.7.2013), the Council of the EU had "regarded to the Treaty on the Functioning of the European Union, and in particular Articles 82(1)(d) and 87(2)(a), in conjunction with Article 218(5) thereof."

²⁰⁶ Opinion of AG Mengozzi, paragraph 108.

²⁰⁷ Article 6(1) of Agreement (12657/5/13 REV 5, 23.6.2014).

[T]he fact nonetheless remain[ed] that...the agreement envisaged [did] not really seem to contribute to facilitating cooperation between the judicial or equivalent authorities of the Member States. [I]t [was] only if the Court were to adopt a more generous interpretation of Article 82(1)(d) TFEU...or if the contracting parties were to amend the terms of the agreement envisaged in such a way that [its] judicial dimension [was] taken more directly into account, that Article 82(1)(d) TFEU might genuinely constitute an additional legal basis for the act concluding that agreement.²⁰⁸

The CJEU adhered to this view.²⁰⁹ The judges acknowledged that the norms of the draft Agreement did not allude to easing collaboration. Besides, the authority appointed by Canada was neither a judicial nor a similar authority.²¹⁰

Considering these remarks, it might appear questionable whether the EU PNR could lawfully be based upon Article 82(1)(d) TFEU. As is explained below, however, this legal basis suffices to justify the adoption of some elements of the Directive.

The type of cooperation foreseen in that provision is present in the PNR Directive as, *inter alia*, it provides for the interchange of PNR data.²¹¹ The authorities competent to first process these data are PIUs. They were not foreseen in the EU-Canada Agreement. PIUs are law enforcement authorities who collect, retain, and analyze the personal data of air passengers that are included by carriers in their PNR receipts.²¹² Each PIU may also exchange raw or processed data with other PIUs and with Europol.²¹³ One of the purposes of the Directive is, thus, to allow for cooperation between law enforcement authorities by means of exchanging data in connection to court procedures in criminal affairs.²¹⁴

There is even a provision specifically on data transfers between the PIUs and other authorities.²¹⁵ This second step is likewise quite relevant. Article 9 determines that PIUs process information to detect individuals who need to be further investigated because they could be involved in terrorism or serious criminal conduct.²¹⁶ Besides, they must respond to duly justified requests from authorized entities to assess and supply PNR information in particular situations for the purposes of the Directive.²¹⁷

²⁰⁸ Opinion of AG Mengozzi, paragraph 108.

²⁰⁹ Opinion 1/15, paragraph 102.

²¹⁰ *Idem*, paragraph 103.

²¹¹ Article 1(1)(b) of Directive (EU) 2016/681, *in fine*.

²¹² Article 4(2)(a) of Directive (EU) 2016/681.

²¹³ Article 4(1) of Directive (EU) 2016/681.

²¹⁴ Article 82(1)(d) TFEU.

²¹⁵ Title of Article 9 of Directive (EU) 2016/681.

²¹⁶ Article 6(2)(a) of Directive (EU) 2016/681.

²¹⁷ Article 6(2)(b) of Directive (EU) 2016/681.

According to Article 7 of Directive (EU) 2016/681, PIUs are established or designated by the member states, who then notify the Commission of their choices.²¹⁸ They must be competent to prevent, detect, investigate, or prosecute terrorist or serious criminal acts.²¹⁹ For now, they range from courts to national and local police, ministerial sections, military forces, secret services, and border agencies.²²⁰ Many of the authorities mentioned in the lists sent by the member states to the Commission are judicial authorities. Others can be considered equivalent authorities, like the PIUs themselves, although this could be a matter of debate.

There is no definition of what a judicial or equivalent authority is, in treaty law. It might be quite a stretch to consider some of those entities as equivalent to judicial authorities, and to thus claim that the Directive is sufficiently limited to the scope of Article 82(1)(d). Besides, the TFEU does not use this expression elsewhere. Since there is no explanation as to what equivalent means, nor about the scope or breadth of this concept, the Union legislator has interpreted it in a broad way, finding that authorities competent for law enforcement purposes, specifically in relation to criminal matters, are within the scope of the expression ‘equivalent authorities’ of Article 82(1)(d).

Although Article 7 of the Directive and the other provisions referring to the PIUs do not talk specifically about judicial and equivalent authorities, all of them must be competent to scrutinize PNR receipts and to take the necessary measures to serve the purposes of the Directive.²²¹ It is, therefore, possible to find a connection between the intra-EU PNR and this treaty law basis, even if the former could have been worded more clearly.

Some help can be found in recital (23), which stresses that the Directive does not prevent or encroach upon the transfer of data between law enforcement and judicial bodies by means of other EU legal tools. The word ‘other’ shows that the legislator finds PNR to be one of the instruments in law enforcement cooperation based on the exchange of data. Plus, recital (23) also says that the rules governing police and judicial collaboration apply to the sharing of data.

The legislator has further claimed that only an EU-wide PNR scheme allows for real collaboration between local agencies.²²² Besides, Article 6(4) specifies that processing standards must be defined and periodically checked by the PIUs in coordination with the other

²¹⁸ Article 7(3) of Directive (EU) 2016/681.

²¹⁹ Article 7(2) of Directive (EU) 2016/681.

²²⁰ Notice from member states on the list of competent authorities referred to in Article 7 of 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 (OJ C 194, 6.6.2018), with the corrigenda present in OJ C 220, 25.6.2018 and OJ C 344, 26.9.2018.

²²¹ Articles 7(1) and (2) of Directive (EU) 2016/681, read together.

²²² Recital (35) of Directive (EU) 2016/681.

authorities of the member states. And Article 9(5) adds that data transfers can take place by resorting to any mechanisms of communication used by the authorities.

Unlike the Agreement, the PNR Directive promotes cooperation between judicial and equivalent authorities. The elements that refer to cooperation, transfers of data, and the very purpose of the system, *inter alia*, are correctly based on this legal basis. Moreover, given that the Commission is informed by the member states about the identity of these entities, it can be argued that the Directive does not leave the choice of authorities, or the processing of PNR, exclusively in the hands of the member states. If the member states were to allow data to be transferred to authorities outside the scope of Article 7, this would give rise to non-compliance with the Directive and allow the Commission to pursue an infringement action against the relevant member state.

It would be interesting to know whether all the authorities chosen by the member states so far are judicial or equivalent, and what would happen if they went beyond Article 7 and allowed authorities that are not thus to access and process PNR. However, these questions are not crucial to ascertaining the matter of legal bases from the perspective of the thesis. They go beyond the purpose of this research and are therefore not going to be explored further.

1.2 Article 87(2)(a) TFEU

The grounds for the second treaty basis mentioned in the Directive, Article 87(2)(a) TFEU, are shakier. Included in the chapter on police cooperation, Article 87(1) enables the Union to launch mechanisms of cooperation including police units, border control, and even specialized services. For this purpose, Article 87(2)(a) empowers the Council and the EP, through the ordinary legislative procedure, to define policies based on “the collection, storage, processing, analysis and exchange of relevant information.”²²³

The Court also considered this legal basis in Opinion 1/15. Here, the judges discussed the content and purpose of the Agreement and then its connection with the TFEU.²²⁴ They found that given that PNR data were to be transferred to Canada to prevent, detect, investigate, and prosecute serious international offenses and terrorism, the envisaged Agreement indeed referred to the purposes laid out in Article 87(1) and was within the scope of Article 87(2)(a).²²⁵ Following the Opinion of the AG, the CJEU further remarked that PNR data being originally

²²³ Article 87(2)(a) TFEU.

²²⁴ Opinion 1/15, paragraphs 95 ff.

²²⁵ *Idem*, paragraph 100.

obtained by carriers for their business rather than by law enforcement authorities for criminal investigations did not prevent Article 87(2)(a) from serving as an adequate legal basis.²²⁶ What is more, it claimed that:

[T]he terms ‘processing’ and ‘exchange’ of such data cover both its transfer to the Member States’ competent authorities in this area and its use by those authorities. In those circumstances, measures concerning the transfer of personal data to competent authorities in relation to the prevention, detection and investigation of criminal offences and the processing of that data by those same authorities fall within the scope of the police cooperation referred to in Article 87(2)(a) TFEU and may be based on that provision.²²⁷

Despite the collection of data being undertaken by private actors, it is clear that the Court considers that the purpose for which such information is used and the nature of the entities which process it are the relevant criteria for determining the appropriateness of the selected legal basis. In light of this case law, the subject-matter and scope of the PNR Directive might appear to fit under Article 87(2)(a) TFEU. Its Article 1 states that it “provides for...the transfer by air carriers of passenger name record (PNR) data [and] the processing of the data[,] including its collection, use[,] retention...and its exchange between Member States[,] for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime.”²²⁸

However, there is an aspect that needs to be better explored in relation to Article 87(2)(a). This concerns the reference to “relevant information.”²²⁹ In its judgement, the Court simply mentioned that relevant data could comprise personal data.²³⁰ Yet, this appraisal is superficial, leaving open questions about its meaning in this context.

The CJEU knew that all passenger data were to be transferred to Canada. This can be inferred immediately from the fact it concluded that the Agreement was invalid due to a lack of clarity about which data could be transferred and processed. It would only have been considered valid, from this point of view, if the text defined the information to be sent to outside the EU in a clear and precise way.²³¹ This remark is very pertinent to the discussion on the proportionality of PNR systems. It will be revisited later in the thesis precisely for this purpose. Yet, it is also useful for illuminating the limits and meaning of Article 87(2)(a) TFEU, *in fine*, as a legal basis for the Directive.

²²⁶ Opinion 1/15, paragraph 101.

²²⁷ *Idem*, paragraph 99.

²²⁸ Articles 1(1) and (2) of Directive (EU) 2016/681, read together.

²²⁹ Article 87(2)(a) TFEU, *in fine*.

²³⁰ Opinion 1/15, paragraph 99.

²³¹ *Idem*, paragraph 232(3)(a).

PNR receipts created under the Directive may contain all the personal data elements of all air passengers regarding all bookings of all flights crossing EU borders.²³² There are no criteria to sort through data and there has been no institutional assessment justifying the need to harvest all these data, or demonstrating how they are relevant for the purposes of the Directive.

From its wording, however, it does not seem that Article 87(2)(a) provides *carte blanche*, permitting the indiscriminate retention of all kinds of big data, especially of a personal nature. On the contrary, it is written in such a way as to oblige the legislator to pass secondary law allowing only for the collection of those data which are relevant for the security purposes set out in secondary legislation.

It appears, therefore, that the Directive allows for the broad retention and use of data beyond what treaty law permits. In fact, only some of its provisions are limited in a way which respects that threshold. Article 6(2)(b), for example, tables guarantees limiting data transfers from the PIUs to other competent authorities and to Europol. One of such guarantees is that these entities should be provided only with the byproduct of data processing operations.²³³ This means that other entities are to receive PNR receipts after they have been treated and assessed by the PIUs, instead of all the information originally sent by carriers. These data are, therefore, limited to the relevant elements that competent authorities and Europol will need to carry out their law enforcement operations.

It is true the PIUs probably need to receive large troves of raw data to ascertain what is relevant for their law enforcement purposes, and what is not. Yet, perhaps there could be less information contained in the PNR receipts, or some of it could be eliminated once passengers are cleared by the PIUs. Maria Tzanou raises doubts about whether many of the data items retained are really necessary.²³⁴ There are many alternatives the legislator could have considered to mitigate, or altogether avoid, the collection of so much data. Law enforcement authorities do not need them to achieve the purposes of the Directive. This is especially the case regarding data that are redundant in identifying passengers or in tracking their movements. In fact, the legislator should have studied alternative options to ensure only the processing and retention of relevant information, thus respecting the principle of data minimization and fully complying with Article 87(2)(a).

²³² Article 3, item (5), and Annex I of Directive (EU) 2016/681.

²³³ Article 6(2)(b) of Directive (EU) 2016/681.

²³⁴ Tzanou, 2017: 171.

1.3 The missing Article 16 TFEU

One of the questions submitted by the EP to the CJEU on the validity of the EU-Canada PNR Agreement concerned the issue of whether Articles 82(1)(d) and 87(2)(a) TFEU constituted a sufficient legal base for the Council to settle the Agreement, or whether it ought also to be grounded on Article 16 TFEU.²³⁵ In the view of the EP, the Council should have taken into consideration this latter provision, since it affects the AFSJ, as well as all areas of Union law.²³⁶ This was justified because the Agreement substantially concerned data protection.²³⁷

The CJEU partially agreed with the EP. It thought that Article 16 should have been one of the legal bases explicitly mentioned in the Council decision on the conclusion of the EU-Canada Agreement, together with Article 87(2)(a) TFEU. However, it did not concede that it would be possible to conclude the Agreement based on Article 16 alone.²³⁸

Since the rise of the CFREU to the status of primary law, Article 16 has often been set aside. This is due to its similarity with Article 8 CFREU and the more detailed nature of this latter provision.²³⁹ Yet, Article 16 TFEU should continue to enjoy some of the spotlight,²⁴⁰ not least as a legal basis for secondary law provisions. Article 16(1) states that “[e]veryone has the right to the protection of personal data concerning them.”²⁴¹ And Article 16(2) reads that:

The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.²⁴²

²³⁵ Opinion 1/15, paragraph 1.

²³⁶ *Idem*, paragraph 32.

²³⁷ *Idem*, paragraph 33.

²³⁸ *Idem*, paragraph 232(1).

²³⁹ Article 8 CFREU reads that “1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.”

²⁴⁰ Other entities have likewise underlined the relevance of Article 16 TFEU as a legal basis for the decision to conclude the PNR Agreement, in observations submitted to the CJEU. The Council and the Commission, for instance, argued that it “would constitute the appropriate legal basis for an act...where the principal objective of that act is the protection of personal data” (Opinion 1/15, paragraph 48).

²⁴¹ Article 16(1) TFEU.

²⁴² Article 16(2), 1st paragraph, TFEU. Its 2nd paragraph adds that “[t]he rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 [TEU].” This norm foresees a procedural change, whereby the Council can legislate alone on matters pertaining to the Common Foreign and Security Policy. It states that “[i]n accordance with Article 16 [TFEU] and by way of derogation from paragraph 2 thereof, the

The CJEU claimed that the Agreement foresaw a set of norms aimed at safeguarding personal data.²⁴³ In fact, it appeared to have two main purposes, one concerning the need to guarantee public security and a second one to do with the safety of information.²⁴⁴ The judges acknowledged that the first purpose was the leading one.²⁴⁵ However, they argued that the Agreement likewise contained many substantive provisions meant to ensure that the content of PNR receipts was safe and protected when they were transferred to Canada.²⁴⁶

As such, the Court held that concluding the Agreement was explicitly linked to the aim foreseen by Article 16(2) TFEU.²⁴⁷ And it added that:

That provision constitutes...an appropriate legal basis where the protection of personal data is one of the essential aims or components of the rules adopted by the EU legislature, including those falling within the scope of the adoption of measures covered by the provisions of the [TFEU] relating to judicial cooperation in criminal matters and police cooperation.²⁴⁸

The judges therefore ruled that, beyond Article 87(2)(a),²⁴⁹ Article 16 must also be one of the legal bases supporting the decision to settle the Agreement.²⁵⁰ If this is the case for the PNR Agreement,²⁵¹ the Directive should similarly be based on that provision, since it also has as one of its essential aims or components the protection of personal data, as will be shown below.

As with the Agreement, the intra-EU PNR often refers to the protection of data. It does not begin by saying that its goal is to establish the means through which personal data will be secure.²⁵² Yet, other provisions indicate that this is one of its key purposes. Each PIU must appoint a Data Protection Officer (DPO), for instance, who will oversee the management of information and put in place appropriate protections.²⁵³ Positive matches must always be

Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.”

²⁴³ Opinion 1/15, paragraph 89.

²⁴⁴ *Idem*, paragraph 90.

²⁴⁵ *Idem*, paragraph 91.

²⁴⁶ *Idem*, paragraph 92.

²⁴⁷ *Idem*, paragraph 95.

²⁴⁸ *Idem*, paragraph 96.

²⁴⁹ *Idem*, paragraph 98.

²⁵⁰ *Idem*, paragraph 97. See also paragraph 104.

²⁵¹ Article 16 TFEU would, consequently, be expressly included as a substantive legal basis, together with Article 87(2)(a) TFEU, in the opening remarks of Recommendation for a Council Decision (COM(2017) 605 final, 18.10.2017).

²⁵² Article 1 of Agreement (12657/5/13 REV 5, 23.6.2014).

²⁵³ Article 5(1) of Directive (EU) 2016/681.

examined by non-automatic means on an individual basis,²⁵⁴ and DPOs should be able to access all stored information in the PIUs, as well as having the autonomy to file complaints to national supervisors if they suspect infringements.²⁵⁵ Besides, PIUs must keep and process PNR receipts solely in secure settings within EU borders.²⁵⁶

On the other hand, data are safeguarded by access limitations, like mandatory requests to the PIUs,²⁵⁷ or compulsory conditions to allow transfers to the Europol²⁵⁸ and third countries.²⁵⁹ There are also guarantees about depersonalization and the retention period,²⁶⁰ as well as a specific norm on data protection. Article 13 provides for individual data rights, prohibits negative discrimination based on sensitive data, obliges PIUs to document all operations, and foresees mechanisms to deal with security breaches.

Regardless of the efficacy of these norms, they suffice to show that, as with the Canada Agreement, data protection is an important objective or component as per the wording of Article 16 in the intra-EU PNR Directive. This does not mean its guarantees are adequate, or sufficient, to protect fundamental rights. The claim here is simply that the Directive should have been based in Article 16 TFEU as well.

This raises a problem, however, the solution to which is not as linear as in the case of Article 87(2)(a) TFEU. While it is relatively safe to say that secondary law provisions going beyond their treaty law bases are unlawful, it is not so easy to make such a claim when the legislator fails to include a necessary legal basis.

The Court concluded, in Opinion 1/15, that the Agreement had to be based both on Article 16(2) and 87(2)(a) TFEU.²⁶¹ It appears that, in PNR systems, keeping data safe is not an incidental objective but is as essential a purpose as police cooperation through the processing of relevant information to prevent, detect, and investigate criminal offenses. So, does this mean the Agreement was invalid because Article 16 TFEU was not expressly included among the legal bases relied on in the Council decision? And if this is so, can the Directive be considered unlawful for likewise not referring to this provision?

²⁵⁴ Article 6(5) of Directive (EU) 2016/681.

²⁵⁵ Article 6(7) of Directive (EU) 2016/681.

²⁵⁶ Article 6(8) of Directive (EU) 2016/681.

²⁵⁷ Article 6(2)(b) of Directive (EU) 2016/681.

²⁵⁸ Article 10 of Directive (EU) 2016/681.

²⁵⁹ Article 11 of Directive (EU) 2016/681.

²⁶⁰ Article 12 of Directive (EU) 2016/681.

²⁶¹ Opinion 1/15, paragraph 232.

It seems the answer to these questions is yes. As the case law of the CJEU shows,²⁶² the key issue is to determine whether data protection is an important, or just incidental, objective of the PNR Directive. Considering that it is as relevant as the fight against crime and that they cannot be dissociated, in light of Opinion 1/15, the lack of a basis in Article 16 TFEU makes the intra-EU PNR scheme insufficiently grounded.

The Court may soon address these questions again, as there are already requests for preliminary rulings questioning the validity of the Directive, which allude to the lack of Article 16 among its legal bases.²⁶³ The judges did not say which bits of the Agreement should be covered by this provision. Yet, if it concerns the protection of data, it is reasonable to assume two things. In the first place, Article 16 forces the EU legislator to include provisions guaranteeing the safety and integrity of data in every legal act that foresees data processing systems used for law enforcement cooperation. The other side of this coin is that the legislator can only include these data protection norms because Article 16 permits it. Without this reference to Article 16, there is no primary law basis sustaining data protection norms in secondary law on judicial and police cooperation.

This is the reason why the GDPR, for example, is specifically based on Article 16. One of its essential aims or components is the protection of personal data. And this is also why the 2014 PNR Agreement and the 2016 PNR Directive should have been based on Article 16 TFEU. The provisions foreseeing data protection guarantees in the intra-EU PNR, like those mentioned above, could only have been validly included in the Directive if Article 16 had been expressly set out as a legal basis. As with the Agreement, Articles 82 and 87 are not sufficient legal bases taken alone.

²⁶² See the parallelism in case C-42/97, *European Parliament v Council of the European Union*, 23 February 1999 (ECLI:EU:C:1999:81), paragraph 38 (which mentions case C-300/89, *Commission of the European Communities v Council of the European Communities*, 11 June 1991 (ECLI:EU:C:1991:244), paragraph 13). Case C-42/97 says that it must be seen “whether culture [was] an essential component of the contested decision, in the same way as industry, and [could not] be dissociated from industry, or whether the ‘centre of gravity’ of the decision [was] to be found in the industrial aspect of the Community action” (paragraph 43). Case C-336/00, *Republik Österreich v Martin Huber*, 19 September 2002 (ECLI:EU:C:2002:509), paragraph 31, adds that “if it is established that the act simultaneously pursues a number of objectives, indissociably linked, without one being secondary and indirect in relation to the other, such an act may be founded on the various corresponding legal bases” (which mentions Opinion 2/00, paragraph 23).

²⁶³ See, for instance, Request for a preliminary ruling in case C-817/19, *Ligue des droits humains*, 31 October 2019, paragraph 47.

2. Limits to competence creep

The EU legislator did not only legislate beyond what Article 87(2)(a) TFEU allows. This second part builds on and extends this argument. It will be claimed that the legislator also acted beyond the conferred powers of the Union, since it overlooked certain treaty law limits applicable to its legislative competences in the AFSJ.

The EU and its member states share competences in the AFSJ.²⁶⁴ Yet, no treaty has entirely settled the matter of the limits and balance between the powers conferred on the Union and the original security powers that remain with the member states. There is already considerable literature on competence creep and limitation of powers. This part does not enter into general discussions. It will, instead, engage with scholars who focus on national security exceptions, develop their ideas, and use them to challenge the validity of the intra-EU PNR system.

2.1 A long story short

The Union has knitted a complex web of policies and laws on security. Following the approval of the Schengen acquis,²⁶⁵ the Treaty of Maastricht²⁶⁶ considered judicial and police cooperation²⁶⁷ to be matters of common interest to the member states. Originally, the CJEU thought that, in principle, criminal and criminal procedure law were subjects under the responsibility of the member states.²⁶⁸ Yet, its jurisprudence²⁶⁹ has been steadily nurturing the idea that EU law also imposes certain restrictions.²⁷⁰

Primary law was, back then, taking its first steps in establishing shared competences on criminal law, security, and law enforcement. This helps to explain why Article K.2(2) of the Treaty of Maastricht foresaw an exception to the growing EU powers, which tried to keep some

²⁶⁴ Piris, 2010: 75.

²⁶⁵ Schengen Agreement of 14 June 1985 between the Governments of the states of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, last modified by Regulation (EC) 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 381, 28.12.2006).

²⁶⁶ Treaty on European Union (OJ C 191, 29.7.1992).

²⁶⁷ Articles K.1(7) and K.1(9), respectively.

²⁶⁸ Case C-203/80, *Criminal proceedings against Guerrino Casati*, 11 November 1981 (ECLI:EU:C:1981:261), paragraph 27.

²⁶⁹ See cases C-186/87, *Ian William Cowan v Trésor public*, 2 February 1989 (ECLI:EU:C:1989:47), paragraph 19, C-226/97, *Criminal proceedings against Johannes Martinus Lemmens*, 16 June 1998 (ECLI:EU:C:1998:296), paragraph 19, and C-61/11 PPU, *Hassen El Dridi, alias Soufi Karim*, 28 April 2011 (ECLI:EU:C:2011:268), paragraphs 53 and 54.

²⁷⁰ Case C-203/80, paragraph 27.

degree of control under the grasp of the member states. This norm provided that the rules on cooperation in the fields of justice and home affairs did “not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security.”²⁷¹ This security exception has resisted the test of time, becoming Article 72 TFEU.

The Declaration on the future of the Union attached to the Treaty of Nice²⁷² was crucial for EU competence. It laid down key issues, such as the definition and monitoring of the allocation of powers between member states and the EU.²⁷³ The contracting parties intended to outline a real limit to competence creep at institutional level.²⁷⁴

In December 2001, the European Council meeting in Laeken addressed the issue of EU competences, recognizing it as one of the challenges in EU reform. It was stressed that the Union had to be more democratic, effective, and transparent.²⁷⁵ Processes for defining and allocating competences were found to be unclear. The Presidency believed citizens would be closer to the Union if its conferred powers were well-defined. As such, it was suggested that forthcoming meetings should debate how each future EU policy was framed within the scope of its competences.

The European Council even recommended a competence re-assignment. In the future, the Union should consider whether it wants to take a more comprehensive approach to cooperation in criminal justice matters.²⁷⁶ The future of the EP was likewise examined. The key issue was whether national parliaments should have a say in the sharing of competences.²⁷⁷ This would be discussed as well in the Convention on the Future of the Union,²⁷⁸ where a competence reform started to take shape. These changes would be later included in the Treaty of Lisbon.²⁷⁹

²⁷¹ Article K.2(2) of the Treaty of Maastricht.

²⁷² Declaration 23 to the Treaty of Nice amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts (OJ C 80, 10.3.2001).

²⁷³ Paragraph 5, 1st item, of Declaration 23 to the Treaty of Nice.

²⁷⁴ De Witte, 2017: 67. This would also happen in the negotiations of subsequent treaties, according to Hijmans & Scirocco, 2009: 1496.

²⁷⁵ Annex I ‘Laeken Declaration on the future of the European Union,’ 4.

²⁷⁶ *Idem*, 5.

²⁷⁷ *Idem*, 6.

²⁷⁸ The Convention took place from February 2002 to July 2003, assembling 105 members, including representatives from member states, EU institutions, and third countries that had applied to join the EU. The first part was dedicated to listing the needs and aspirations of citizens and member states, which would be subsequently studied and prepared for discussion in a second phase. By the end of 2002, several working groups put forward their results and recommendations and the Convention used them to draft the Treaty establishing a Constitution for Europe (OJ 2004/C 310, 16.12.2004).

²⁷⁹ De Witte, 2017: 67.

2.2 The Lisbon *status quo* on security

Security is a core attribute of statehood²⁸⁰ and a tool of political and legal authority.²⁸¹ This means that state power is the legal foundation for national security.²⁸² Such ideas have influenced EU treaty law, which is between a rock and a hard place in trying to find a compromise that enables the Union to achieve its objectives in the AFSJ, while still affording some agency for the member states to regulate and oversee their national security agendas.

The Treaty of Lisbon has not escaped this predicament. It is divided between allowing national security to be the sole responsibility of the member states, and fostering a robust AFSJ. On the one hand, Article 4(2) TEU, *in fine*, claims that “national security remains the sole responsibility of each Member State.”²⁸³ On the other, Article 4(2)(j) TFEU states that “[s]hared competence between the Union and the Member States applies in the...area of freedom, security and justice.”²⁸⁴ The treaty does not define the concepts of security, or national security. Neither does it set their boundaries.

In the meanwhile, the EU has been expanding its security powers²⁸⁵ by, *inter alia*, enacting binding legal acts, like the PNR Directive. This has been justified by a growing number of threats of a transnational nature, terrorism first and foremost. These threats have led Union institutions to argue that these matters can only be efficiently addressed through international and regional cooperation under the EU umbrella.²⁸⁶

This position was hardened as the Union acquired legal personality,²⁸⁷ and a body to be secured,²⁸⁸ with Lisbon. It seems that, nowadays, member states are only free to decide

²⁸⁰ For Harding, 2015: 2, the proximity between authority and core societal values is what gives a sensitive character to criminal law and matters of public security. If a state loses part of its legislative powers in the field, the society can also lose part of its common identity. Therefore, in legal and political terms, allocating or abdicating from security sovereignty is a delicate and contentious topic.

²⁸¹ This can be seen in the slow beginnings of EU policymaking on security. The measures undertaken in the 1980's and 1990's were considerably limited because security was still perceived as being a matter of member state competence. It was, therefore, not a top priority on the Union agenda. See Casagran, 2015: 243, and O'Neill, 2012: 18.

²⁸² Enerstvedt, 2014: 28. See also Article 1.2 of Guidelines on Passenger Name Record (PNR) data.

²⁸³ Article 4(2) TEU.

²⁸⁴ Article 4(2)(j) TFEU.

²⁸⁵ In contrast, see Barros, 2012: 518, who argues that “most counter-terrorism responsibilities remain within the hands of the Member States. The new EU involvement does not entail a transfer of competences from Member States to the EU, as the EU does not hold any exclusive competence in counter-terrorism.” Servent & MacKenzie, 2011: 391, likewise claim that there are severe limitations on EU competence and what the Union can do on counter-terrorism. This might have been true back then, but the evolution of secondary legislation and EU powers on security proves otherwise.

²⁸⁶ It is true that security, nowadays, requires different capabilities and involves numerous actors who need to cooperate. However, they also tend to compete in these “[n]etwork politics” (Pawlak, 2009: 562).

²⁸⁷ Article 47 TEU.

²⁸⁸ Hampton, 2013: 78.

exclusively regarding mutual assistance in cases of terrorism, or armed offenses.²⁸⁹ Abraham Newman anticipated that Lisbon would “communitarize”²⁹⁰ many aspects of internal security and law enforcement collaboration. Other authors, however, have not been so quick to take the member states out of the equation. Ben Jones thinks European security lacks teeth while a proper defense strategy is not implemented.²⁹¹ And Antonio Manrique de Luna Barrios adds that countries still decide individually about most military interventions,²⁹² usually under the North Atlantic Treaty Organization.²⁹³

What is, at least, clear is that, since 2009, EU law has been extending its reach to areas that were previously under national jurisdiction.²⁹⁴ By abolishing the pillar system, security has come to be under European influence,²⁹⁵ in a single institutional frame.²⁹⁶ While some authors, like Jörg Monar, still see the treaties as rather protective of national powers,²⁹⁷ their arguments seem tenuous in light of the growing Union intervention in security and law enforcement.

The fear of competence creep has, nevertheless, persisted. The aforementioned Article 4(2) TEU, *in fine*, is a clear example that member states are not always willing to hand over their competences to the EU.²⁹⁸ Loïc Azoulai highlights that one of the idiosyncrasies of the Treaty of Lisbon is, indeed, the plethora of norms restricting EU competences.²⁹⁹ And André Klip has even argued that Lisbon has given more relevance to national identities and member states’ security responsibilities than previous treaties.³⁰⁰

This is why Paul Craig and Gráinne De Búrca suggest that the AFSJ is designed in a rather particular way.³⁰¹ EU norms are necessary to ensure joint transnational action and the enforcement of common values. While in many areas of shared competences there is, nonetheless, a considerable margin of discretion for the member states, the AFSJ has been an

²⁸⁹ Which results from the solidarity clause, present in Article 222 TFEU.

²⁹⁰ Newman, 2011: 498.

²⁹¹ Jones, 2011: 44.

²⁹² The challenge of coordinating peace operations, like in Bosnia-Herzegovina, mirrors the difficulties in assembling a single EU voice (Manrique de Luna Barrios, 2017: 305).

²⁹³ For some literature, the EU is a clear sponsor of defense, but it is not an active participant, since it is the member states who decide about most actions and policies. These authors recognize that international cooperation is essential for European visibility, but still see the Union as a civilizing agent, mostly a soft power with a humanitarian agenda (Pérez de las Heras, 2017: 366).

²⁹⁴ Rosas & Armati, 2018: 182.

²⁹⁵ Passible of “comunitarización,” in the original Spanish (Molina del Pozo & Mata Diz, 2013: 57). See also Saulnier-Cassia, 2017: 208.

²⁹⁶ Salminen, 2011: 298.

²⁹⁷ Monar, 2011: 559.

²⁹⁸ Hijmans & Scirocco, 2009: 1496, 1497, and 1522.

²⁹⁹ Azoulai, 2011: 196.

³⁰⁰ Klip, 2016: 37.

³⁰¹ Craig & De Búrca, 2015: 973.

exception. A fast “‘Europeanisation’ of internal security”³⁰² is taking place, with more and more security policies being strongly influenced by the Union.

The security *status quo* after Lisbon is not easy to describe, let alone comprehend. What is clear is that there is a tension in EU law between the provisions regulating the AFSJ, and those idiosyncrasies that limit the Union’s security competences. The edges of conferral and the scope of national security exceptions are still far from well-defined.³⁰³ This has given rise to countless debates, as well as criticism of how the AFSJ is being built. Janne Salminen, for instance, believes that treaty provisions on police cooperation expect secondary law to be limited to minimum norms.³⁰⁴ Differently, Takis Tridimas argues that the EU cannot even legislate on national security.³⁰⁵

PNR is one of the most recent policies illustrating the Union’s creeping competences in security. It reveals a proactive EU legislator which should have drafted the Directive in such a way as to leave more scope for the member states to decide on certain issues that directly conflict with how they manage their national security agendas. In fact, some of those national security exceptions seem to apply to PNR, and the member states should have retained some of those responsibilities that fall within the PNR system.

2.3 Applicable national security exceptions

By enacting a Directive so detailed that it resembles a Regulation,³⁰⁶ the Union left little margin of discretion for the parliaments and governments of the member states to have a voice in PNR, and it weakened their stance in internal security. In the first place, and despite the harmonization goals pursued by the EU, PNR systems are so intrusive into the lives of air passengers and the

³⁰² Monar, 2011: 560.

³⁰³ *Idem*: 559.

³⁰⁴ Salminen, 2011: 291.

³⁰⁵ Tridimas, 2012: 57.

³⁰⁶ This is a classic topic of discussion that is gaining ground since legislation enacted by the Union is rapidly harmonizing criminal and criminal procedure law (Mitsilegas, 2010: 460). As this author claims, based on Articles 82(2), 83(1) and (2), and 288, 3rd paragraph, TFEU, “Directives leave Member States a considerable margin of manoeuvre as to how to implement EU law, being binding as to the result to be achieved but leaving to the national authorities the choice of form and methods. This discretion left to Member States may serve to take into account the particularities of their domestic criminal justice systems when called to implement EU measures...It is clear that Member States [prefer] such discretion rather than for top-down uniform standards across the EU.” The problem is that Directive (EU) 2016/681 hardly fits this definition. It leaves little margin of discretion for member states to make decisions about PNR, national authorities have almost no voice in the form and methods of implementation, and the particularities of their domestic criminal and constitutional systems have barely been taken into account. This is a problem common to many directives, which occurs because the EU has been approving directives over the years with norms as specific and as comprehensive as those contained in regulations. This serves mainly to guarantee that directives are effective, but it comes with the cost of gravely limiting the discretion that member states enjoy (Hartley, 2014: 223).

business of carriers that they should be an optional security feature whose implementation is left to the discretion of the member states.³⁰⁷ Instead, the Union opted for a “top-down uniform”³⁰⁸ legislation whereby “implementation is, from the Member State’s point of view, an empty exercise.”³⁰⁹

As already mentioned, this part of the chapter will try to establish that the Union was not competent to adopt a fully-fledged intra-EU system, due to the national security exceptions contained in the treaties and that, by doing so, the Directive is liable to be declared invalid. With a mandatory PNR system almost fully outlined at the European level, the Union is forcing the member states to collect, retain, process, and possibly transfer all the personal data from all air passengers crossing their borders to an unprecedented degree. They are required to do so regardless of their constitutional and legal traditions, security agendas, or attitudes towards fundamental rights.

It can be argued that the Directive disregards what treaty law says about the responsibilities of the member states on security. The EU legislator should have limited its content to harmonizing data transfers, defining messaging formats and safe channels of communication, and to ensuring that fundamental rights and EU data protection laws were respected by the member states, if they were to decide autonomously to implement national PNR schemes.

As noted earlier, there are two national security exceptions in the treaties that can be used to question how far the EU legislator is entitled to interfere with the responsibilities of the member states on security and, therefore, to challenge the validity of the Directive. To reiterate, these are found in Articles 72 TFEU and 4(2) TEU, *in fine*. Scholars have also called them competence reservation clauses, although considering the first to be a direct derogation clause and the second a general exception to the principle of conferral. This is because Article 72 is included in the title V of the TFEU, which regulates the AFSJ, and Article 4 is one of the common provisions opening the TEU. While the former is perceived as a specific brake in the system, the latter is seen as a general principle guiding EU action on a broader scale. Authors

³⁰⁷ It could be argued that the member states were co-legislators in the process, thus having all the necessary margin to exercise their responsibilities and powers. Yet, this codecision mechanism is far from what the drafters of the treaties intended regarding national security exceptions, or any exception to EU competence creep. In light of this caveat in primary law, allowing for member states to decide, at Union level, on proposals submitted by the Commission, in areas of exclusive or shared competences, does not satisfy the requirement of empowering national parliaments to legislate by themselves, or having member states retain exclusive responsibilities. National security exceptions point towards letting them model their legal systems according to their societal needs and contexts. It is true that member states had an important share of responsibility in approving the Directive, both directly at the Council of the EU and through the MEPs. Still, this does not compare to having them design and implement key features of the system internally, through a truly harmonized and cooperative effort.

³⁰⁸ Mitsilegas, 2010: 460.

³⁰⁹ Hartley, 2014: 223.

are seldom clear on the merits of such categorization and why they use it. Since it is of little relevance for the present research, they will simply be considered national security exceptions, as the EP named them.³¹⁰

These exceptions do not prevent the Union from legislating on security matters, or from furthering the goals of the AFSJ. It is established in the jurisprudence of the CJEU that considerations of national security cannot be used to try to prevent the enforcement of EU law.³¹¹ The judges have repeated the idea that, while it is the responsibility of the member states to take the necessary steps to guarantee their security, both internally and externally, this does not mean that those steps are completely beyond the scope of Union law,³¹² even regarding national measures³¹³ taken “for the purpose of protecting national security,”³¹⁴ “public security or national defence.”³¹⁵ Regardless of the criticism that can be made of the fact that the Court has not accepted that all measures affecting national security fall beyond the reach of EU law, this jurisprudence has the merit of making it clear that only in extraordinary and very well-defined situations can actions undertaken by the member states be regarded as falling within a national security exception and, consequently, as outside the scope of the EU.³¹⁶ And it is for EU law to decide on which those situations are.

³¹⁰ Although Article 4(2) TEU and 72 TFEU are similar in terms of substantive content, the literature singles out the former from other competence clauses. From the academic discussions, it is possible to identify three main reasons for this. In the first place, Article 4(2) is in the TEU and not the TFEU. It is more a foundational and institutional rule than a procedural, or technical, norm. It is among other “general provisions on the foundations of EU integration and of the EU legal order” (Klamert, 2019 (a): 5). Secondly, it is shaped as one of the principles that “lay down a framework governing the functioning and the operation of the Union” (Klamert, 2019 (a): 5), instead of as a direct command that constraints the EU or member states to act, or to abstain from acting, in certain situations. Finally, it applies to the whole structure of the Union as it appears in the opening provisions of the TEU, and not in the specific title of the TFEU on the AFSJ. It is not a feature associated with a concrete field of primary law, but a general instruction horizontal to EU action.

³¹¹ Klamert, 2019 (b): 45.

³¹² Case C-38/06, *European Commission v Portuguese Republic*, 4 March 2010 (ECLI:EU:C:2010:108), paragraph 62.

³¹³ See, for instance, case C-252/01, *Commission of the European Communities v Kingdom of Belgium*, 16 October 2003 (ECLI:EU:C:2003:547), paragraph 30.

³¹⁴ Cases C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*, 6 October 2020 (ECLI:EU:C:2020:790), paragraph 44 (which mentions cases C-300/11, *ZZ v Secretary of State for the Home Department*, 4 June 2013 (ECLI:EU:C:2013:363), paragraph 38, C-178/16, *European Commission v Republic of Austria*, 20 March 2018 (ECLI:EU:C:2018:194), paragraphs 75 and 76, and C-715/17, C-718/17 and C-719/17, *European Commission v Republic of Poland and Others*, 2 April 2020 (ECLI:EU:C:2020:257), paragraphs 143 and 170), and C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others v Premier ministre and Others*, 6 October 2020 (ECLI:EU:C:2020:791), paragraph 99.

³¹⁵ Case C-337/05, *Commission of the European Communities v Italian Republic*, 8 April 2008 (ECLI:EU:C:2008:203), paragraph 42.

³¹⁶ Cases C-273/97, *Angela Maria Sirdar v The Army Board and Secretary of State for Defence*, 26 October 1999 (ECLI:EU:C:1999:523), paragraph 16, C-285/98, *Tanja Kreil v Bundesrepublik Deutschland*, 11 January 2000 (ECLI:EU:C:2000:2), paragraph 16, and C-461/05, *European Commission v Kingdom of Denmark*, 15 December 2009 (ECLI:EU:C:2009:783), paragraph 51. Analogously, see case C-222/84, *Marguerite Johnston v Chief Constable of the Royal Ulster Constabulary*, 15 May 1986 (ECLI:EU:C:1986:206), paragraph 26.

This stems immediately from the very existence of an AFSJ, an area of law and policy to be built co-operatively between the Union and the member states. In fact, for the Court, admitting, as a general principle, that any action taken by the member states motivated by concerns of public security could be outside the range of EU law, beyond very specific occasions, would jeopardize the compulsory nature and equal application of EU law.³¹⁷ This comes in line with the Court's belief that internal security cannot be seen as isolated, as it is inextricably related to the overall security of the international community.³¹⁸

What national security exceptions aim at is, in contrast, to limit how far, under cover of shared competences, EU law encroaches upon a core of member states' responsibilities in relation to their national security agendas and policies. Though the AFSJ is constructed in a way that gives preference to the Union to regulate and harmonize security, potentially to the detriment of the national security interests of the member states, the drafters of the treaties do not appear to have wanted an AFSJ fully decided at EU level. These national security exceptions, together with the sharing of competences, are a reminder that this should be a collaborative effort wherein the member states retain some of their original powers to decide, not the least, regarding foundational aspects of their security programs.

Despite this, the Union has been legislating on security with few, if any, constraints. This has been possible for two reasons. In the first place, many of the provisions foreseeing national security exceptions are ambiguous, or contradictory in light of other norms.³¹⁹ Some of them have had, in fact, more political echo than normative strength,³²⁰ like Article 4(2) TEU, *in fine*. Secondly, as demonstrated, the CJEU has taken advantage of this legal uncertainty to affirm the EU's sway over security matters. Based on the argument that the member states are not generally free to deviate from the treaties solely on the basis of their security interests,³²¹ the Court has curtailed their agency in the AFSJ.³²² Its interpretation of Article 72 TFEU, as will be seen below, is an example of how it has reduced the scope and strength of certain exceptions.

³¹⁷ Case C-38/06, paragraph 62.

³¹⁸ Case C-70/94, *Fritz Werner Industrie-Ausrüstungen GmbH v Federal Republic of Germany*, 17 October 1995 (ECLI:EU:C:1995:328), paragraph 26, which was copied from Opinion of AG Francis Jacobs, delivered on 18 May 1995 (ECLI:EU:C:1995:151), paragraph 46.

³¹⁹ Molina del Pozo & Mata Diz, 2013: 52.

³²⁰ Craig, 2010: 347.

³²¹ Case C-387/05, *European Commission v Italian Republic*, 15 December 2009 (ECLI:EU:C:2009:781), paragraph 47.

³²² In case C-105/03, *Criminal proceedings against Maria Pupino*, 16 June 2005 (ECLI:EU:C:2005:386), paragraph 42, the CJEU found that "[i]t would be difficult for the Union to carry out its task effectively if the principle of loyal cooperation, requiring in particular that Member States take all appropriate measures, whether general or particular, to ensure fulfilment of their obligations under European Union law, were not also binding in the area of police and judicial cooperation in criminal matters, which is moreover entirely based on cooperation between the Member States and the institutions." This was inspired by Opinion of AG Juliane Kokott, delivered

This interpretation has found some resonance in the literature. Marcus Klamert, for instance, claims that only when treaty law provides for specific derogations, can member states oppose the scope of EU law. Following a certain body of jurisprudence,³²³ he believes that, beyond these derogations, the Union is under no duty to prioritize the national interests of the member states over its own interests.³²⁴ These derogations are present in Articles 36, 45, 52, 65, 72, 346, and 347 TFEU.³²⁵ Curiously, however, Klamert has ignored other Court rulings where some of these derogations have been limited or emptied of legal meaning, like Article 72 TFEU.

The following sections will analyze the national security exceptions that are relevant to discussions regarding the intra-EU PNR. Although Articles 72 TFEU and 4(2) TEU, *in fine*, have similar wording, they have distinct useful content. It will be argued that the former has been emptied of its legal strength and cannot be used to question interference by the Union in the national security agendas and policies of the member states.

2.3.1 Article 72 TFEU

Article 72 TFEU states that the provisions in the AFSJ “shall not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security.”³²⁶ This provision comes from previous treaties.³²⁷ As will be explored below, the Directive contains recitals referring explicitly to internal security and its scope and subject matter are clearly within the logic of Article 72 and the maintenance of law and order.

on 11 November 2004 (ECLI:EU:C:2004:712), paragraph 26. She argued that “Article 1 EU lays down the objective of creating a new stage in the process of achieving an ever closer union among the peoples of Europe, on the basis of which relations between the Member States and between their peoples can be organised in a manner demonstrating consistency and solidarity. That objective will not be achieved unless the Member States and institutions of the Union cooperate sincerely and in compliance with the law. Loyal cooperation between the Member States and the institutions is also the central purpose of Title VI of the Treaty on European Union, appearing both in the title — Provisions on Police and Judicial *Cooperation* in Criminal Matters — and again in almost all the articles.”

³²³ In concrete, case C-38/06 read together with cases C-300/11, paragraph 38, and C-387/05, paragraph 45.

³²⁴ Klamert, 2019 (b): 45.

³²⁵ Article 36 concerns “restrictions on imports, exports or goods in transit,” Article 45 is about “limitations [to the] freedom of movement for workers,” Article 52 regards restrictions to the right of establishment, and special treatment, “for foreign nationals,” and Article 65 talks about how member states may “take measures which are justified” to restrict the movement of capital between them and with third countries. Articles 346 and 347 deviate from this pattern. The former refers to the “supply [of] information the disclosure of which [the member state] considers contrary to the essential interests of its security,” and the latter to cooperation to “prevent the functioning of the internal market being affected by measures which a Member State may be called upon to take” in extraordinary circumstances. They are not relevant to discussions regarding PNR, unlike Article 72, which is assessed in depth in this chapter.

³²⁶ Article 72 TFEU.

³²⁷ “Article 33 EU, Art 64(1) EC” (Craig, 2010: 347). See also Mitsilegas, 2010: 461, and Kellerbauer, 2019: 791.

Paul Craig argues that this provision fails to “reflect reality,”³²⁸ since it promises more than it can deliver. The design of the AFSJ does not make very clear what such responsibilities of member states may be. As Craig points out, competences are shared in the AFSJ. This means that Union action will unavoidably limit the responsibilities of member states in keeping law and order. For him, what matters is how the nature and extent of this limitation differ depending on the action undertaken by the EU.

It is hard to envisage the maintenance of law and order in member states as falling outside the scope of EU law, given that the TFEU proclaims that the Union should maintain a high degree of security by taking steps to deter and fight crime, as well as by coordinating and fostering collaboration between law enforcement agencies.³²⁹ The useful content of Article 72 is lessened, from the outset, by this incongruity.

Some scholars, like Manuel Kellerbauer, think that this “public order clause...should be construed narrowly.”³³⁰ There seems, indeed, to be few other ways to read Article 72. Still, it is worth taking a close look at it to see whether it may be useful for critiquing the creeping competences of the EU that have been revealed with the approval of PNR.

The first step is to interpret Article 72, namely by defining the concept of internal security and checking whether the scope of the PNR Directive overlaps with it. The following step is to see what the Court has written on this provision. Article 72 has been largely depleted of its normative strength and, consequently, has limited value for the present research. In light of the current interpretation of Article 72 by the CJEU, it is doubtful whether member states can challenge the validity of the Directive based on this provision. It raises, in any event, interesting questions for contemplating national security exceptions and their dialogue with secondary law on the AFSJ.

A. Defining internal security

By stating that the member states are responsible for maintaining law and order and for preserving their internal security, it looks like Article 72 TFEU is bringing these concepts into proximity. Maintaining law and order is part of what it means to safeguard internal security, even though the treaties fail to define it. The vocabulary of security is, oddly, not very clear in

³²⁸ Craig, 2010: 347.

³²⁹ Article 67(3) TFEU.

³³⁰ Kellerbauer, 2019: 791.

primary law, which has given rise to a certain confusion in the case law, scholarly writing, and discussions within EU institutions.

Albeit that it is often used interchangeably with the notion of public security, the CJEU has also referred to public security as comprising both the internal and the external aspects of security.³³¹ They appear to be two sides of the same coin.

External security essentially means military defense. This was established already in 1999, when the Court claimed that the organization of the armed forces and recruitment for the military service are within the sphere of competences of the member states.³³² The judges said that member states should implement effective actions to guarantee security, internally and externally, and organize their military.³³³ Curiously, they later added that this did not mean that their actions were completely beyond the scope of EU law.³³⁴

External also relates to border control. While ruling in a case about the elimination of internal borders in Regulation (EC) 562/2006,³³⁵ the CJEU argued that national police forces exercising their powers under municipal law must be regarded differently from border control.³³⁶

In a report following the adoption of the Treaty of Lisbon, the House of Lords of the United Kingdom suggested that internal security should be understood in a minimalistic way. It considered that this expression refers to matters of public order to be handled internally by member states, especially those under the jurisdiction of police forces.³³⁷ Nonetheless, the

³³¹ Case C-367/89, *Criminal proceedings against Aimé Richardt and Les Accessoires Scientifiques SNC*, 4 October 1991 (ECLI:EU:C:1991:376), paragraph 22.

³³² This was the position of Germany already in case C-285/98, paragraph 12. It argued that “Community law does not in principle govern matters of defence, which form part of the field of common foreign and security policy and which remain within the Member States’ sphere of [sovereignty].”

³³³ Case C-273/97, paragraphs 15 and 17. The idea of internal and external security was present in previous decisions, namely cases C-70/94, paragraph 25, and C-83/94, *Criminal proceedings against Peter Leifer, Reinhold Otto Krauskopf and Otto Holzer*, 17 October 1995 (ECLI:EU:C:1995:329), paragraphs 26 and 35. Subsequent decisions would reiterate it, like cases C-423/98, *Alfredo Albore*, 13 July 2000 (ECLI:EU:C:2000:401), paragraph 18, and C-145/09, *Land Baden-Württemberg v Panagiotis Tsakouridis*, 23 November 2010 (ECLI:EU:C:2010:708), paragraph 43.

³³⁴ Case C-273/97, paragraph 15. See also cases C-186/01, *Alexander Dory v Bundesrepublik Deutschland*, 11 March 2003 (ECLI:EU:C:2003:146), paragraphs 24 and 29 to 31. France stressed that decisions on the organization of compulsory military services relate “to national defence, [which is] within the exclusive competence of the Member States” (paragraph 26). The CJEU agreed and added that Union interference to deal with “adverse consequences for access to employment [would encroach] on the competences of the Member States” (paragraph 41).

³³⁵ Later repealed by Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ L 77, 23.3.2016).

³³⁶ Case C-278/12 PPU, *Atiqullah Adil v Minister voor Immigratie, Integratie en Asiel*, 19 July 2012 (ECLI:EU:C:2012:508), paragraph 53. See also case C-9/16, *Criminal proceedings against A*, 21 June 2017 (ECLI:EU:C:2017:483), paragraphs 33 ff.

³³⁷ European Union Committee of the House of Lords, 2008, paragraph 6.238.

Lords regretted that there was no agreed catalogue of matters that fall under the different types of security.³³⁸

Internal security therefore seems to concern law enforcement and police operations. To recall, Article 1(2) of the PNR Directive states that “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.”³³⁹ For Henri Labayle, Article 72 reflects a specific aspect of the AFSJ by foreseeing a stack of powers in the hands of the member states on criminal affairs.³⁴⁰ Hermann-Josef Blanke considers these “reservations to integration”³⁴¹ to be a rather distinct element.³⁴² He believes that, as a result, the state “remains the principal guarantor of security and enforcer of the law as conceived by classical political philosophers such as *Bodin*, *Hobbes* and *Weber*.”³⁴³ Still, Blanke concedes that internal, like national security, is not an exclusive prerogative of the member states. They are not competent to deal with these matters in such a way as to prevent the Union from exercising its sovereignty.³⁴⁴

This strengthens the idea that internal security is, indeed, a matter of shared powers, competences, and responsibilities, not least due to the numerous rules which make the Union competent to legislate on police action and law enforcement.³⁴⁵

B. Weakened provision

Article 72 TFEU has been explored by the Court. On many occasions, it has been the intervening parties who have highlighted the issue pertaining to the scope of security.³⁴⁶ One of the first cases in which the judges discussed the concept of internal security, albeit using the

³³⁸ European Union Committee of the House of Lords, 2008, paragraph 6.241.

³³⁹ Article 1(2) of Directive (EU) 2016/681.

³⁴⁰ Labayle, 2016: 34.

³⁴¹ Blanke, 2013: 194.

³⁴² *Idem*: 231.

³⁴³ *Idem*: 229.

³⁴⁴ *Idem*: 231.

³⁴⁵ See, inter alia, Articles 67(3) and 82(2), or the entire chapter 5, on police cooperation, of the title on the AFSJ of the TFEU.

³⁴⁶ In case C-72/83, *Campus Oil Limited and others v Minister for Industry and Energy and others*, 10 July 1984 (ECLI:EU:C:1984:256), 2737, Ireland claimed that member states have a primary competence in public security. It argued that treaty law considers the “concept of «public security» [to be] of a special kind inasmuch as the Community has no competence itself in that field and...the Member States have retained their own powers intact.” This was endorsed by the United Kingdom, who maintained that member states should be free to approve derogative measures under public security “if they are designed to secure a fundamental interest of the State which can properly be protected on that ground...or if they are designed to enable the life of the State to function safely and effectively” (2741 and 2742). A similar position was advocated by Greece when it said that “the maintenance on national territory of a stock of petroleum products allowing continuity of supplies to be guaranteed constitute[d] a public security objective,” in case C-398/98, *Commission of the European Communities v Hellenic Republic*, 25 October 2001 (ECLI:EU:C:2001:565), paragraph 29.

expression ‘public security,’ was in 2012. It concerned the interpretation of Article 28(3) of Directive 2004/38/EC, which reads that “[a]n expulsion decision may not be taken against Union citizens, except if the decision is based on imperative grounds of public security, as defined by Member States.”³⁴⁷

The CJEU acknowledged that member states should be able to specify what they consider to be those imperative grounds.³⁴⁸ However, it immediately added that:

While Member States essentially retain the freedom to determine the requirements of public policy and public security in accordance with their national needs, which can vary from one Member State to another and from one era to another, particularly as justification for a derogation from the fundamental principle of free movement of persons, those requirements must nevertheless be interpreted strictly, so that their scope cannot be determined unilaterally by each Member State without any control by the institutions of the European Union.³⁴⁹

This interpretation has been recalled and reaffirmed in different cases.³⁵⁰ It leaves little doubt as to the position of the Court regarding the scope of Article 72. This view, however, has not been consensual in the literature. Bruno De Witte notes that the Court did not set practical criteria to understand this norm and that it made member states not truly free to define their policies on the limitation of movement.³⁵¹

This reading might be a reaction against Article 276 TFEU, which states that the CJEU “[s]hall have no jurisdiction to review the validity or proportionality of operations carried out by the police or other law-enforcement services of a Member State or the exercise of the

³⁴⁷ Article 28(3)(a) of Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (OJ L 158, 30.4.2004).

³⁴⁸ Case C-348/09, *P.I. v Oberbürgermeisterin der Stadt Remscheid*, 22 May 2012 (ECLI:EU:C:2012:300), paragraph 22.

³⁴⁹ *Idem*, paragraph 23.

³⁵⁰ See, for instance, cases C-41/74, *Yvonne van Duyn v Home Office*, 4 December 1974 (ECLI:EU:C:1974:133), paragraphs 18 ff., C-36/75, *Roland Rutili v Ministre de l'intérieur*, 28 October 1975 (ECLI:EU:C:1975:137), paragraphs 26 and 27, C-30/77, *Régina v Pierre Bouchereau*, 27 October 1977 (ECLI:EU:C:1977:172), paragraphs 33 and 34, C-348/96, *Criminal proceedings against Donatella Calfa*, 19 January 1999 (ECLI:EU:C:1999:6), paragraphs 21 to 23, C-54/99, *Association Eglise de scientologie de Paris and Scientology International Reserves Trust v The Prime Minister*, 14 March 2000 (ECLI:EU:C:2000:124), paragraph 17, C-36/02, *Omega Spielhallen- und Automatenaufstellungs-GmbH v Oberbürgermeisterin der Bundesstadt Bonn*, 14 October 2004 (ECLI:EU:C:2004:614), paragraphs 30 and 31, C-33/07, *Ministerul Administrației și Internelor – Direcția Generală de Pașapoarte București v Gheorghe Jipa*, 10 July 2008 (ECLI:EU:C:2008:396), paragraph 23, C-430/10, *Hristo Gaydarov v Direktor na Glavna direktsia ‘Ohranitelna politsia’ pri Ministerstvo na vatrešnite raboti*, 17 November 2011 (ECLI:EU:C:2011:749), paragraph 32, and C-434/10, *Petar Aladzhov v Zamestnik direktor na Stolichna direktsia na vatrešnite raboti kam Ministerstvo na vatrešnite raboti*, 17 November 2011 (ECLI:EU:C:2011:750), paragraph 34.

³⁵¹ De Witte, 2017: 64.

responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security.”³⁵²

By guaranteeing that there is little, or no, space for member states to exercise any kind of responsibility free from EU interference, the CJEU has eluded this “residual limitation on [its] jurisdiction.”³⁵³ This way, the Union, as a whole, retains a considerable degree of control over local police and law enforcement operations even if the Court, individually, does not. By stretching the reading of Article 72 to its limit, the CJEU has quashed any possible scenario in which there persists a core of member states’ responsibilities free from Union intervention.

C. Insufficient basis to prevent creeping competences

It appears there is no “EU-free zone”³⁵⁴ within the scope of Article 72. There may not be any meaningful legal content to be salvaged which could sustain an argument to prevent the EU legislature from enacting such an exhaustive and detailed intra-EU PNR scheme. It also seems unlikely that the Court would impugn the validity of the PNR Directive for not allowing a margin of discretion to member states to regulate their security systems on this basis. As such, and despite the apparent robustness and clarity of Article 72, its problems render it unusable to prevent the creeping competences of the EU, manifesting with the approval of PNR.

The Directive contains two recitals referring to internal security. Recital (6) says that “[e]ffective use of PNR data...is necessary to prevent, detect, investigate and prosecute terrorist offences and serious crime and thus enhance internal security.”³⁵⁵ And recital (15) claims that:

A list of the PNR data to be obtained by a PIU should be drawn up with the objective of reflecting the legitimate requirements of public authorities to prevent, detect, investigate and prosecute terrorist offences or serious crime, thereby improving internal security within the Union...The PNR data should only contain details of passengers’ reservations and travel itineraries that enable competent authorities to identify air passengers representing a threat to internal security.³⁵⁶

³⁵² Article 276 TFEU. Kellerbauer, 2019: 791, even considers that Articles 72 and 276 TFEU somehow complement each other.

³⁵³ Peers, 2011: 666. See also Salminen, 2011: 292, who thinks that “there has been a conscious decision not to include guarantees of the access to justice of individuals in relation to the evaluation of the validity and proportionality of the activities of police authority. The same applies to evaluating the extent to which Member states fulfil their responsibilities in maintaining law and order and internal security, even though in principle access to justice would be especially necessary in these questions.”

³⁵⁴ De Witte, 2017: 64.

³⁵⁵ Recital (6) of Directive (EU) 2016/681.

³⁵⁶ Recital (15) of Directive (EU) 2016/681.

It is not exactly clear whether recital (6) refers to internal security from the perspective of the member states or of the Union. It could be seen as the former, since the recital talks about operations undertaken by national law enforcement authorities. Recital (15), on its side, refers first to the Union's internal security and, then, possibly, to the member states', as threats are to be identified by national competent authorities.

PNR serves to safeguard both the internal security of the member states and the Union as a whole. This is clear in those recitals and from the general purposes of the Directive. The information collected is to be processed to prevent, detect, investigate, and prosecute terrorism and serious transnational crimes.³⁵⁷ The criminal offenses it lists³⁵⁸ pertain to the logic of internal security, being investigated, primarily, by law enforcement units.

Given the structural problem of Article 72 TFEU, the powers of the Union on police matters, and the case law of the CJEU, it seems this provision has lost most of its legal strength. Thus, it cannot be safely claimed that the EU legislature, in enacting PNR, went beyond its conferred powers based on Article 72. As things stand, this provision does not preserve a core of state powers on internal security in the hands of member states and free from EU interference. It is not a national security exception which can be mobilized against the intra-EU PNR system.

2.3.2 Article 4(2) TEU, *in fine*

Article 4(1) TEU states that "competences not conferred upon the Union in the Treaties remain with the Member States"³⁵⁹ and the principle of conferral³⁶⁰ is developed in Article 5. The EU has only the competences that treaty law, and, therefore, the member states, have given it.³⁶¹ This is especially important regarding security, since it is a crucial building block of statehood.

Notwithstanding Article 4(2)(j) TFEU determining that the AFSJ is an area of shared competences, Article 4(2) TEU appears to foresee a national security exception to this sharing of power. It reads that:

The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State,

³⁵⁷ Article 1(2) of Directive (EU) 2016/681.

³⁵⁸ Annex II of Directive (EU) 2016/681.

³⁵⁹ Article 4(1) TEU.

³⁶⁰ Klamert, 2019 (b): 38.

³⁶¹ Tridimas, 2012: 50.

maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.³⁶²

This provision originated in efforts undertaken while preparing the Constitutional Treaty of 2004, to mitigate the effects that functional powers were having on those policy areas which the member states deem more delicate.³⁶³ It is known as the Christophersen clause, after Henning Christophersen, the Danish delegate at the Convention on the future of the European Union, at Laeken, in 2001, who was especially involved in its drafting.³⁶⁴

The security exception appears in the last sentence. As with many other exceptions scattered in the treaties, this provision creates quite an impact on first reading. A literal interpretation could suggest that member states have a large margin of discretion to decide on security, even with regard to issues falling within the scope of the AFSJ. There is room for discussion on the content of the “enigmatic”³⁶⁵ ending of Article 4(2) TEU.

Although the general stance of the CJEU on security exceptions is that the member states cannot invoke a core of sovereignty³⁶⁶ which evades the influence of EU law, its case law has not yet delved deep into the complex world of Article 4(2) TEU, *in fine*. The Court’s silence has provoked a variety of different reactions.

Some scholars claim that this norm sets parameters that work as constitutional chains, casting light on the legitimate scope of EU action and restricting its ability to take over the competences of the member states.³⁶⁷ On the other hand, this silence has created some anxiety regarding the reach of Court rulings which can impact on how member states conduct security. AG Campos Sánchez-Bordona has highlighted the fact that:

³⁶² Article 4(2) TEU. On the principle of subsidiarity and this provision, see Dougan, 2008: 657 ff.

³⁶³ De Witte, 2017: 70.

³⁶⁴ Klamert, 2019 (b): 38. See also Amato & Ziller, 2007: 107 and 108. A primitive version can be found in the Treaty of Maastricht. It would take a shape similar to its current formulation in the Constitutional Treaty to smooth the exercise of EU powers in areas that could be sensitive for member states. Still, its final form is the “product of the Intergovernmental Conference of 2007 that adopted the Lisbon Treaty,” according to Von Bogdandy & Schill, 2011: 1426.

³⁶⁵ De Witte, 2017: 70.

³⁶⁶ *Idem*: 60. The author was testing the argument of Koen Lenaerts, who wrote, back in 1990, that “there simply is no [constitutionally protected] nucleus of sovereignty that the Member State can invoke...against the Community” (Lenaerts, 1990: 220). Though he did not table a rigid interpretation, Lenaerts still stressed that even “when the Treaty expressly acknowledges the existence of residual powers for the Member States,” the nucleus of sovereignty is not impervious. The author illustrated his view with cases C-120/78, *Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein*, 20 February 1979 (ECLI:EU:C:1979:42), C-148/78, *Criminal proceedings against Tullio Ratti*, 5 April 1979 (ECLI:EU:C:1979:110), and C-153/78, *Commission of the European Communities v Federal Republic of Germany*, 12 July 1979 (ECLI:EU:C:1979:194). See also the references to joined cases C-7/56 and C-3/57 to C-7/57, *Dinecke Algeria, Giacomo Cicconardi, Simone Couturaud, Ignazio Genuardi, Félicie Steichen v Common Assembly of the European Coal and Steel Community*, 12 July 1957 (ECLI:EU:C:1957:7), and C-6/69 and 11-69, *Commission of the European Communities v French Republic*, 10 December 1969 (ECLI:EU:C:1969:68).

³⁶⁷ Klamert, 2019 (a): 5.

[A]uthorities in some Member States are concerned by [the] judgments...of 8 April 2014, *Digital Rights Ireland and Others*...21 December 2016, *Tele2 Sverige and Watson and Others* [and] 2 October 2018, *Ministerio Fiscal*...because, in their view, the result is to deprive them of an instrument which they consider essential to the safeguarding of national security and countering terrorism. That is why some of those Member States argue that the case-law in question should be overturned or qualified.³⁶⁸

Until very recently, the judges have mostly limited their observations to stressing the idea mentioned above that Article 4(2) does not contain a wide-ranging rule exempting public security actions from the grasp of EU law.³⁶⁹ This remark reflects the traditional view of the CJEU on security exceptions, even though it leaves ample margin for interpretation. With this observation, it avoided scrutinizing Article 4(2) but managed nonetheless to ensure that member states could not block EU action protecting individuals by invoking a margin of discretion under the indeterminate concept of national security.³⁷⁰ Yet, as will be seen below, there are some recent developments in the case law that have come to help define the meaning of this concept.

Similarly to the above analysis of Article 72 TFEU, the following sections will, first, interpret the substantive legal content of the national security exception present in Article 4(2). The purpose is to table a sensible and meaningful interpretation of the concepts of national security and sole responsibility. It will then be seen whether the legislator went beyond its conferred powers in the AFSJ when it enacted the PNR Directive, in light of this provision. Although there may be deep disagreements about its nature and meaning, it proves a relevant tool for questioning the Union's creeping competences in security, and challenging the validity of the Directive.

³⁶⁸ Opinion of AG Campos Sánchez-Bordona (a), delivered on 15 January 2020 (ECLI:EU:C:2020:5), paragraph 1.

³⁶⁹ Case C-38/06, paragraph 62. This has also been stressed by some AG. See, for instance, Opinion of AG Campos Sánchez-Bordona (a), paragraph 31, where he said that “[n]ational security concerns cannot [be argued so that legislation] would not come within the scope of EU law.” Although talking about national identity, AG Juliane Kokott would later reinforce this. She thinks that “the division of competences between the European Union and its Member States follows from the treaties. The European Union’s obligation under Article 4(2) TEU to respect the national identities of its Member States does not in itself support the inference that certain subject areas or areas of activity are entirely removed from the scope of Directive 2000/78. It requires rather that the *application* of that directive must not adversely affect the national identities of the Member States. National identity does not therefore limit the scope of the Directive as such, but must be duly taken into account in the interpretation of the principle of equal treatment which it contains and of the grounds of justification for any differences of treatment” (Opinion of AG Juliane Kokott, delivered on 31 May 2016 (ECLI:EU:C:2016:382), paragraph 32).

³⁷⁰ Opinion of AG Campos Sánchez-Bordona (b), delivered on 15 January 2020 (ECLI:EU:C:2020:6), paragraph 74.

A. Difficult interpretation

Interpreting Article 4(2) TEU, *in fine*, requires a considerable effort as it does not adopt the typical terminology of conferral. Clemens Ladenburger has rightly suspected that it would be very difficult to interpret,³⁷¹ ever since the approval of the Treaty of Lisbon.

Janne Salminen claims that most EU competences are defined in the treaties in a clear way, especially regarding police and judicial cooperation.³⁷² Yet, the vocabulary used in Article 4(2) is anything but clear. For one thing, it does not set a sharp limit that can be used by courts, member states, and EU institutions to assess the interference of Union law with the national security responsibilities of the member states. For another, the meaning of national security and sole responsibility in the logic of conferral is rather ambiguous. Each of these points will be discussed in turn below.

A.1 National security

No definition of national security is mentioned in treaty law. To understand this concept for the purposes of EU law is a difficult task that requires some digging. Despite the complexity of this section, the overall relevance of this discussion for PNR will become clear in the end.

Safeguarding national security is vital for states,³⁷³ just like “ensuring [their] territorial integrity [and] maintaining law and order.”³⁷⁴ These are examples of areas about which member states are exceptionally concerned.³⁷⁵ National security does not depend on the constitutional identity of states. Blanke says it relates, instead, to the “very «identity as a State»...as it refers not to a particular national interpretation, but to *the State* as a general concept.”³⁷⁶ It objectively reveals statehood.³⁷⁷ The essence of statehood foreseen in the treaties is intimately tied to the use of force, which is normally under state control.³⁷⁸

The use of force as a key feature of national security has also been highlighted by the German Constitutional Court. In 2009, it claimed that any handover of sovereignty that goes beyond intergovernmental collaboration and affects fundamental rights can only aim at harmonization,

³⁷¹ Ladenburger, 2008: 36.

³⁷² Salminen, 2011: 282.

³⁷³ Klamert, 2019 (b): 45.

³⁷⁴ Article 4(2) TEU.

³⁷⁵ De Witte, 2017: 70.

³⁷⁶ Blanke, 2013: 228. See also Cantaro, 2006: 510 ff.

³⁷⁷ Ibidem.

³⁷⁸ Ibidem.

take place in certain transnational circumstances, and be restricted by specific conditions. The principle is that member states must remain free to act and to decide on security.³⁷⁹

Still, there are so many diverging interpretations of what security means that even some AGs have failed to sharpen the scope and differences between national, public, and state security. For Sánchez-Bordona, for instance, they have overlapping meanings, based on his reading of Article 1(3) of Directive 2002/58/EC.³⁸⁰ This provision states that it “shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as...activities concerning public security, defence, State security...and the activities of the State in areas of criminal law.”³⁸¹ Moreover, its Article 15(1) permits member states to enact legislation to “safeguard national security (i.e. State security), defence, public security.”³⁸²

He has elsewhere written that collecting and using data is essential to “countering serious threats to public security, particularly terrorism, espionage and nuclear proliferation. The [United Kingdom Security and Intelligence Agencies’] capabilities to acquire and use the data are essential to the protection of the national security of the United Kingdom.”³⁸³ This acritical use of national and public security needs refining, but it has the merit of being a good starting point for discussing and narrowing the concepts.

A 2014 study of the Directorate-General for internal policies of the EP, on national security and secret evidence, echoes the impression that the notion of national security is opaque and shrouded in legal uncertainty. Although the concept is frequently used in legal and political discussions, both at Union and national level, there is yet no common and clear understanding of what it entails in most member states. And even when they try to define it, it seems that the definitions they propose do not meet the requirements of legal certainty and the rule of law. The study proposed certain actions to tackle this uncertainty, from an EU observatory on this evolving concept, to harmonized local legislation dealing with whistle-blowers.³⁸⁴ This shows how difficult it can be to define national security.

Conflating national, state, and even internal security is common in scholarly writing. Valsamis Mitsilegas has tabled concerns on whether the concepts of national and internal security intersect, or whether the latter should be used to refer to police cooperation and national

³⁷⁹ Judgment of the Second Senate of the German Constitutional Court, *Lisbon*, 2 BvE 2/08, 30 June 2009 (ECLI:DE:BVerfG:2009:es20090630.2bve000208), paragraph 253.

³⁸⁰ Opinion of AG Campos Sánchez-Bordona (b), paragraph 77.

³⁸¹ Article 1(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002).

³⁸² Article 15(1) of Directive 2002/58/EC.

³⁸³ Opinion of AG Campos Sánchez-Bordona (a), paragraph 17. See also paragraphs 20 and 38.

³⁸⁴ Directorate-General for internal policies of the European Parliament, 2014: 7.

security should cover military and intelligence activities.³⁸⁵ Ladenburger has also suggested that national security could be seen simply as regarding intelligence services, excluding any law enforcement action.³⁸⁶

It seems national security is normally associated with complex state affairs, namely counter-terrorism, intelligence, and fighting very serious crime. Its relevance for PNR is thus beginning to take shape, since the Directive provides for the processing of data to counter terrorism and serious crime.³⁸⁷ Yet, to entirely detach this concept from law enforcement measures, like Ladenburger does, might be hasty considering the modern complexity and interoperability of police action. Blanke comments that:

The maintenance of law and order [i.e., internal security] is accompanied by the function of safeguarding national security, which partially overlaps with the notion of public policy (and security)...In some ways it is however even wider, as it also comprises external security. It refers to essential matters affecting the existence of the State.³⁸⁸

The research division of the European Court of Human Rights (ECtHR) produced a document, in 2013, on national security and European case law. It is not a study on EU law, but it may nonetheless be helpful. It is notable that it reinforced this interpretation of national security. It argued that the concept tends to be used in relation to terrorism.³⁸⁹ As in EU treaty law, it is far from clear and may be described as rather ambiguous in the European Convention on Human Rights. The ECtHR has thus been working to make it more concrete, with the research division finding that it unquestionably comprises the defense of states and democracies against acts of separatism, terrorism, espionage, and incitement to infringe military conduct. The report concluded that, at the CoE, state parties have a wide margin of discretion to assess and counter risks to national security.³⁹⁰

Mitsilegas observes that treaty law uses this term mostly from a national standpoint. He goes as far as suggesting that there is no real effort to integrate security into the wider context of the AFSJ.³⁹¹ This is an interesting perspective, although it is not entirely consensual in the literature. Blanke, for instance, argues that national and internal security are, nowadays, terms

³⁸⁵ Mitsilegas, 2010: 461.

³⁸⁶ Ladenburger, 2008: 36.

³⁸⁷ Article 1(2) of Directive (EU) 2016/681.

³⁸⁸ Blanke, 2013: 230, based on case C-72/83, paragraph 34.

³⁸⁹ Research Division of the European Court of Human Rights, 2013: 4.

³⁹⁰ *Idem*: 38.

³⁹¹ Mitsilegas, 2010: 461.

of EU law, but he also believes that member states still retain a margin to develop their internal policies.³⁹² This position, however, seems to clash with the idea that it is for the CJEU to interpret them and their evolving scope in an authoritative manner.

A 2018 briefing from the EP on security claimed that national security is a textbook example of an area that lies beyond the scope of EU law. While there is no single meaning of the concept, the EP acknowledged that it includes measures to fight threats to the member states' "independence, sovereignty, territorial integrity, [and] constitutional order."³⁹³ This interpretation is, nevertheless, rather problematic.

On the one hand, the EP is reducing national security to matters usually associated with external security, i.e., matters of military and external defense. On the other, terrorism and serious criminal offenses can often affect a state's constitutional order, or even its sovereignty. Cybercrime,³⁹⁴ kidnapping and taking key state figures as hostages,³⁹⁵ illicit trafficking in cultural goods³⁹⁶ or nuclear and radioactive materials,³⁹⁷ crimes in the jurisdiction of the International Criminal Court,³⁹⁸ unlawful seizure of aircrafts and ships,³⁹⁹ sabotage,⁴⁰⁰ or industrial espionage⁴⁰¹ are some examples of that type of misconduct. Yet, these examples, which the EP considered to fall beyond the scope of EU law, are examples mentioned explicitly in Annex II of the PNR Directive.

This position of the EP is contradictory. Many of the policies and pieces of legislation enacted by the EP and other institutions in the AFSJ, until 2018 and beyond that, concern terrorist and criminal acts which can affect the "independence, sovereignty, territorial integrity, [and] constitutional order"⁴⁰² of the member states. So, they cannot be outside the scope of EU law. To say they are outside the scope of EU law would be to admit to a blatant violation of conferred powers, well beyond what is being argued in this chapter.

This interpretation of the meaning of national security should be carefully rethought. If it were accepted, the AFSJ would be far more limited than it is, and many legal acts would be invalid. PNR data, for instance, could only be used to investigate some of the criminal offenses that are currently listed in that Annex of the Directive.

³⁹² Blanke, 2013: 231.

³⁹³ European Parliament, 2018: 2.

³⁹⁴ Heading 9 of Annex II of Directive (EU) 2016/681.

³⁹⁵ Heading 14 of Annex II of Directive (EU) 2016/681.

³⁹⁶ Heading 16 of Annex II of Directive (EU) 2016/681.

³⁹⁷ Heading 20 of Annex II of Directive (EU) 2016/681.

³⁹⁸ Heading 22 of Annex II of Directive (EU) 2016/681.

³⁹⁹ Heading 23 of Annex II of Directive (EU) 2016/681.

⁴⁰⁰ Heading 24 of Annex II of Directive (EU) 2016/681.

⁴⁰¹ Heading 26 of Annex II of Directive (EU) 2016/681.

⁴⁰² European Parliament, 2018: 2.

Despite the limited observations of the Court over the last decades, very recent developments in its case law may now help to articulate an authoritative definition of national security. In 2020, the judges admitted having failed to scrutinize “the objective of safeguarding national security”⁴⁰³ before and examined the scope of this concept on two occasions. They appear to mark the beginning of the settling of this matter, albeit the Court is yet to address the thornier question of what ‘sole responsibly’ for member states exactly entails and how competences should be allocated. The CJEU has found that:

[At] the outset...Article 4(2) TEU provides that national security remains the sole responsibility of each Member State. That responsibility corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities.⁴⁰⁴

Save for the aspect of considering national security to lie beyond the scope of EU law, this opinion overlaps with the 2018 briefing of the EP when claiming that national security relates to the protection of the “independence, sovereignty, territorial integrity, [and] constitutional order”⁴⁰⁵ of the member states. The CJEU has drawn a line that separates the notion of national security from related concepts, apparently shattering the conflation of national, public, and internal security. It could have gone further in pulling out the useful content from a sentence as robust as “national security remains the sole responsibility of each Member State.”⁴⁰⁶ Still, this reading strengthens the arguments taking shape in this section and supports the claim that national security is a particular area of state interest that is at the heart of statehood.

The Court added that the “importance of the objective of safeguarding national security, read in the light of Article 4(2) TEU...goes beyond...the objectives of combating crime in general, even serious crime, and of safeguarding public security.”⁴⁰⁷ It has thus acknowledged that treaty law is here protecting the primary interests of the member states that, “by their nature and particular seriousness, [go well beyond] the general risk [of] tensions or disturbances, even of a serious nature, affecting public security.”⁴⁰⁸

⁴⁰³ Joined cases C-511/18, C-512/18 and C-520/18, paragraph 134.

⁴⁰⁴ Cases C-623/17, paragraph 74, and C-511/18, C-512/18 and C-520/18, paragraph 135.

⁴⁰⁵ European Parliament, 2018: 2.

⁴⁰⁶ Cases C-623/17, paragraph 74, and C-511/18, C-512/18 and C-520/18, paragraph 135.

⁴⁰⁷ *Idem*, paragraphs 75 and 136.

⁴⁰⁸ *Ibidem*.

It is now clear that matters of national security are conceptually different from those of internal, external, or public security. And, regardless of whether the Court has relied on it or not, this jurisprudence creates space for the idea that, where EU law regulates matters of terrorism — the only example of criminal activity explicitly mentioned there —, member states must have a degree of agency, a core of responsibility, to be decided at a domestic level, precisely because of the importance of the key interests at play.

This argument can somewhat be glimpsed when the judges said that “[s]ubject to meeting the other requirements laid down in Article 52(1) of the Charter, the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by...other objectives.”⁴⁰⁹ After alerting to the need of complying with the criteria set out in Article 52 CFREU,⁴¹⁰ the sentence highlights how far the legislator and authorities can go to safeguard national security. Seeing that treaty law protects the primary interests of the member states and that national security is one of such fundamental interests, it can thus be suggested that the CJEU is open to consider that their margin of action to decide on matters of national security must be sufficiently wide to ensure that they can safeguard this societal interest effectively. In any case, this aspect of shared responsibilities will be analyzed in more detail in the following section.

Considering the foregoing, especially this recent input from the case law of the CJEU, and keeping in mind the risks of a too narrow definition,⁴¹¹ it seems safe to claim that national security refers to operations countering very serious crime and terrorist acts, as well as to intelligence services and actions relating to state security. For what it is worth, this is likewise supported by the definition present in Encyclopaedia Britannica. It states that national security relates to intelligence and counterintelligence and that, “[i]n continental Europe, police work that is directed at protecting national security is known as high policing, in reference to the «higher» interests of the state.”⁴¹²

This interpretation appears to be the most consensual and sensible. And an important conclusion is that, in this case, the scope of the PNR Directive overlaps with the scope of Article 4(2) TEU. Remembering that PNR data can only be processed to prevent, detect, investigate, and prosecute terrorism and serious offenses, it can be argued that this national security exception applies in the PNR case.

⁴⁰⁹ Case C-623/17, paragraph 75.

⁴¹⁰ See also the criteria laid out in paragraphs 76 ff. of case C-623/17 and 137 ff. of joined cases C-511/18, C-512/18 and C-520/18.

⁴¹¹ European Union Committee of the House of Lords, 2008, paragraph 6.241.

⁴¹² Encyclopaedia Britannica, 2020.

Before moving on, there are two additional remarks that are necessary to bring to the fore at this stage. It may be helpful, on the one hand, to separate this interpretation of national security from the scope and meaning of external security. Article 23(1) of Regulation (EU) 2016/679 says that “Union or Member State law...may restrict by way of a legislative measure the scope of the obligations and rights [of certain provisions] when such a restriction [is] necessary and proportionate...to safeguard (a) national security; (b) defence; (c) public security.”⁴¹³ Military and defense matters are parted from complex crime, terrorism, and intelligence.

The second remark is not so innocuous. It should not be argued that any given operation does not pertain to national security affairs just because it is undertaken by standard law enforcement and police forces. As highlighted above in a comment contra the view of Ladenburger, the level of cooperation between ordinary and special law enforcement units is nowadays so deep and complex that the investigation of serious crime and terrorism can, partially or in full, be handled by the police and similar competent authorities. This does not make such matters less relevant from the viewpoint of the national security agendas of member states. National security is a term related more to the level of complexity of crime and the interests affected, rather than the actors involved in its deterrence.

The CJEU has, nonetheless, twisted this argument to, again, repeat its opinion that EU law applies to any security-related activity. In the recent case law mentioned above, the judges have also affirmed that while there may have been more room for competent authorities to act exclusively under national laws in the past, under the current EU legislation on data protection, “all operations processing personal data [concerning] public security, defence, [and] State security [and including those] resulting from obligations imposed on [private] providers by the public authorities...fall within the scope”⁴¹⁴ of EU law. As such, while processing undertaken by private actors will generally fall within the scope of the GDPR,⁴¹⁵ the data operations performed by public bodies will essentially fall within the scope of Directive (EU) 2016/680,⁴¹⁶ if no other norms apply.

While the Court’s reasoning in this recent case law does not undermine the conclusions tabled before on the content and meaning of national security, it is surprising that the CJEU still feels the need to reiterate such an opinion, as if it feared Article 4(2) TEU. This only continues to create confusion on the normative strength of this provision. Regardless the actors involved

⁴¹³ Article 23(1) of Regulation (EU) 2016/679.

⁴¹⁴ Cases C-623/17, paragraph 46, and C-511/18, C-512/18 and C-520/18, paragraph 101.

⁴¹⁵ *Idem*, paragraphs 47 and 102.

⁴¹⁶ *Idem*, paragraphs 48 and 103.

in data processing, “national legislation enabling a State authority [or] providers of...services to [process or handle] data...for the purpose of safeguarding national security falls within the scope of”⁴¹⁷ EU law.

This reasoning also does not encroach upon the more general point defended in this chapter since the implementation of PNR at European level is not put into question. The concern expressed regards the adoption of a fully-fledged and highly intrusive system. Still, the persistence of the Court fosters a reflection on how far it is willing to go in security integration and on what operational core is truly subject to member state agency and independent decision-making. The next section will help to shed some light on this complex task.

A.2 Sole responsibility

To grasp what the TEU means when it says that member states are solely responsible for national security is an even thornier task. There is little consensus in the literature, with scholars adopting conflicting views and positions that do not fully align with the logic of conferral. So far, the scarce observations of the CJEU have confirmed the predictions of Ladenburger when he claimed that the judges would probably not be capable of exploring the full consequences of Article 4(2) in the way that its drafters expected.⁴¹⁸

Some authors address its national security exception too literally, focusing on the powers apparently maintained in the hands of the member states. For Takis Tridimas, this norm sets out an area of exclusive member state power.⁴¹⁹ He echoes Ladenburger, for whom it contains “a reservation of exclusive national competence”⁴²⁰ that is unique in treaty law. Even AG Sánchez-Bordona has suggested that EU law does not apply to member state action in national security.⁴²¹ In the end, this would mean that:

[T]he EU cannot legislate in this area under any legal basis. It does not, however, remove national security from the dormant competence of the EU. National measures which seek to maintain national security may not interfere with the fundamental freedoms and, insofar as they fall within the scope of EU law, must respect fundamental rights as understood in the EU legal order.⁴²²

⁴¹⁷ Case C-623/17, paragraph 49. See, similarly, joined cases C-511/18, C-512/18 and C-520/18, paragraph 104.

⁴¹⁸ Ladenburger, 2008: 36.

⁴¹⁹ Tridimas, 2012: 57.

⁴²⁰ Ladenburger, 2008: 36.

⁴²¹ Opinion of AG Campos Sánchez-Bordona (a), paragraph 84.

⁴²² Tridimas, 2012: 57.

Other authors have adopted a softer tone, even if they embrace the same perspective. Rosas and Armati, for example, find a core of legislative discretion in this provision.⁴²³ And Armin Von Bogdandy and Stephan Schill believe it tries to guarantee that the Union recognizes key member states' competences.⁴²⁴

A different faction of scholars sees it more as a norm guiding EU action, instead of a clause on member state competence. Blanke affirms that, while reasons of national security may serve to limit the EU when exercising its competences, they are not universal sovereignty reservations and should not be misinterpreted as allowing the member states to exercise exclusive powers.⁴²⁵ Valsamis Mitsilegas sees here a threshold to EU legislative competences on security.⁴²⁶ And Sacha Garben says that Article 4(2) actually entails a control mechanism on competence creep.⁴²⁷ Although the exact legal meaning of that norm is as yet unknown, she thinks that it aims at forcing the Union to uphold national variety, as well as to respect key constitutional elements of the member states.⁴²⁸

Bruno De Witte has built on top of this, arguing that Article 4(2) seems like a red line for the Union to control its interference in the area, rather than a reservation of sovereignty in the hands of the member states.⁴²⁹ For De Witte, it could never be read as a provision on “genuinely exclusive Member State competence [nor] a genuine competence reservation clause.”⁴³⁰ As referred above, the dogmatic differences between these doctrinal perspectives are not going to be explored. Yet, as Article 4(2) does not use the typical language of conferral, it seems sensible to say that its national security exception is not a competence reservation clause but, indeed, an obligation for the EU when legislating on security. The only missing step in this interpretation is about its practical consequences. Authors have failed to suggest what can be extracted from this norm in terms of member states' agency in regulating national security matters.

The intra-EU PNR is an example of a piece of legislation in which the Union should have felt compelled to respect the substantive obligation discussed by De Witte. Article 4(2) TEU should serve, precisely, to make the Union legislator refrain from legislating on security as intrusively as it has done in recent decades. In contrast to this, however, the PNR Directive

⁴²³ Rosas & Armati, 2018: 20 and 21.

⁴²⁴ Von Bogdandy & Schill, 2011: 1426.

⁴²⁵ Blanke, 2013: 231.

⁴²⁶ Mitsilegas, 2010: 461.

⁴²⁷ Garben, 2015: 58.

⁴²⁸ This is also the understanding of Salminen, 2011: 289, who argues that “[t]he question of what added value, in the final analysis, is gained from these provisions...which affect the unit as a whole, is open to broader interpretation.”

⁴²⁹ De Witte, 2017: 70.

⁴³⁰ *Idem*: 72.

stands as a good example of the Union's creeping competences and the frail agency of the member states in the AFSJ.

Michael Dougan is right in claiming that Article 4(2) TEU, *in fine*, has an "open-ended nature (combined with a good dose of institutional connivance)."⁴³¹ By not adopting the classic terminology used in EU law on the division of competences, the drafters have clouded the legal scope and strength of the norm. They, perhaps, feared that keeping security powers explicitly in the hands of the member states could lead to friction in the construction of the AFSJ. Yet, the solution adopted poses challenges, and it is important to recall that, with the Lisbon reform, the allocation of competences in criminal law matters is subject to a set of requirements.⁴³²

Sole responsibility appears to relate more to constitutional law.⁴³³ What is certain is that this provision cannot be interpreted literally. To do so is not defensible, since it goes against other treaty norms which bestow upon the Union competences in national security in the logic of the AFSJ.⁴³⁴ Sole responsibility is certainly not an adequate term. If security is a matter of shared powers and competences, there cannot be responsibilities exercised by the member states in isolation. However, it is also unsustainable to claim that this norm is effective because it is possible for the member states to leave the Union and restore all the powers they had delegated to the Union.⁴³⁵ It cannot be reasonable that this provision is rendered useful only in extremis.

The national security exception in this norm has thus been neglected over the years, mainly due to the difficulties in its interpretation.⁴³⁶ Hitherto, its legal potential seems quite significant, not the least as a mechanism that could help member states challenge the validity of EU secondary law which they consider to be excessively intrusive with respect to their national security agendas. Sole responsibility can be construed in a way that salvages this potential. On the one hand, Article 4(2) should be understood as a substantive obligation that limits EU laws and policies. The Union must supervise its legal output and remind itself that it must cooperate with the member states when legislating on serious crime and terrorism, as well as on intelligence services and actions relating to state security. It should verify that it has done so, for example, by ensuring respect for a strict reason giving requirement.

⁴³¹ Dougan, 2008: 654.

⁴³² Mitsilegas, 2010: 462.

⁴³³ The principle of conferral and this duty to respect national identities stem from the constitutional principles and norms of the member states, according to the judgement of the German Constitutional Court *Lisbon*, paragraph 234.

⁴³⁴ De Witte, 2017: 72.

⁴³⁵ *Idem*: 73.

⁴³⁶ There are very few cases where the CJEU talks about Article 4(2) TEU, *in fine*. The judges do not explore it in detail and tend simply to claim, as seen above, that the member states cannot derogate from EU law while protecting national security. See joined cases C-715/17, C-718/17 and C-719/17, paragraphs 170 ff., and C-808/18, *European Commission v Hungary*, 17 December 2020 (ECLI:EU:C:2020:1029), paragraph 262.

This goes beyond the strict logic of conferral. It is justified by the special relevance of security for state building, which the treaties tried to capture in Article 4(2) and other security exceptions.⁴³⁷ As mentioned by the German Constitutional Court, EU law on these matters should be limited to allowing transnational collaboration and harmonizing exceptional cases.⁴³⁸

This interpretation is also supported when reading together Articles 4(2) TEU and 67(1) TFEU, which reads that “[t]he Union shall constitute an area of freedom, security and justice with respect for fundamental rights and the different legal systems and traditions of the Member States.”⁴³⁹ Mitsilegas sees here the “first, horizontal, element revealing resistance to communautarisation.”⁴⁴⁰ He is right in claiming that respecting national differences has been, from the start, at the heart of the AFSJ.

On the other hand, self-scrutiny may not be sufficient. Alexandros Kargopoulos argues that Article 4(2) should be used to guarantee that the constitutional framework of the member states is respected and that EU secondary law and policies can be challenged if they violate this obligation. The CJEU and the courts in the member states, especially constitutional courts, cannot evade affirming the cooperative logic permeating the AFSJ. They are key players in making this norm legally pertinent and in pulling out the strength of national security exceptions, even if this means quashing EU secondary law. In fact, Article 4(2) seems to call for its own proportionality test to check whether Union law goes beyond those purposes of multilevel harmonization and cooperation. It fosters the “need for a ‘balancing test’ for the resolution of frictions between antithetical precepts of constitutional law and EU law.”⁴⁴¹ If the courts take that step, it will be a step towards making the spirit of the treaties a reality.

Kargopoulos goes so far as to say that this means that lawmakers in the member states have a broader margin to fine-tune EU secondary law on security and criminal affairs than in other areas in which the Union can intervene.⁴⁴² As such, he concludes that breaching such

⁴³⁷ In the judgment of the Polish Constitutional Court *Poland’s membership in the European Union (the Accession Treaty)*, 11 May 2005 (K 18/04), paragraph 15, the judges highlighted that “[t]he Communities and the European Union function, in accordance with the Treaties establishing these organisations, on the basis of, and within the limits of, the powers conferred upon them by the Member States. Consequently, the Communities and their institutions may only operate within the scope envisaged by the provisions of the Treaties. The Member States maintain the right to assess whether or not, in issuing particular legal provisions, the Community (Union) legislative organs acted within the delegated competences and in accordance with the principles of subsidiarity and proportionality. Should the adoption of provisions infringe these frameworks, the principle of the precedence of Community law fails to apply with respect to such provisions.”

⁴³⁸ Judgment of the German Constitutional Court *Lisbon*, paragraph 253.

⁴³⁹ Article 67(1) TFEU.

⁴⁴⁰ Mitsilegas, 2010: 459.

⁴⁴¹ Kargopoulos, 2016: 143.

⁴⁴² *Idem*: 144.

obligations could be considered a sufficient basis to ask for the annulment or non-enforcement of national laws applying European policies.

This is not an easy step, but it is an imperative step in the direction of achieving legal certainty and security that is long due. Mary Dobbs explains why this is not yet standard practice. She recalls that the Treaty of Lisbon:

[D]eveloped in a context where the tension between the Member States and the EU remained unresolved and in part as a reaction to the failure of the Constitutional Treaty. It clarifies and amends some aspects, but unsurprisingly leaves much still unresolved regarding the relationship between the EU and the Member States, with reactions at the national level reflecting the continuing battle over sovereignty, including elements such as primacy.⁴⁴³

A truly cooperative construction of the AFSJ, which values national security exceptions, is still precluded by this battle over sovereignty and by a kind of institutional fear of what member states might do if the principle of conferral and the division of security competences are interpreted in a more nuanced fashion. Yet, these nuances are gaining momentum in the tension between “the categorical positions of the ECJ [supporting] the doctrine of absolute primacy of EU law...and that of most domestic constitutional courts...which largely follow a doctrine of relative primacy.”⁴⁴⁴

Only by having a self-aware and restrained EU, which gives member states a certain leeway regarding the details of national security arrangements and their constitutional identity, and by making this Article 4(2) usable in court, will this norm gain legal significance. Neither the Union nor the member states are solely responsible for national security. That is the very premise of the AFSJ. Still, the latter must keep a certain degree of agency with regard to their security needs, to be assessed on a case-by-case basis. Otherwise, Article 4(2) TEU, *in fine*, is nothing but an empty shell.

As mentioned above, this interpretation of Article 4 may be more in line with the intentions of the drafters of the treaties. It salvages the legal meaning and content of this provision, making it a tool in the hands of the member states to judge, on a case-by-case basis, many EU pre-emptive security policies. The final section of this chapter undertakes such an assessment, with regard to the intra-EU PNR system.

⁴⁴³ Dobbs, 2014: 314.

⁴⁴⁴ Von Bogdandy & Schill, 2011: 1418.

B. PNR beyond conferral

Adding to the claims made in the first part of this chapter, a final contention is that PNR is susceptible to being invalidated because the Union legislator ignored Article 4(2) TEU, *in fine*, and interfered with a core of national security responsibilities that should have been left for the member states to decide upon. There are relevant aspects of the system that the member states could regulate in cooperation with the EU. As things stand, they have little margin of discretion. The Union went beyond its conferred powers in light of the shared competences in the AFSJ and the national security exception of Article 4(2).

There is no mention of national security in the Directive. There are only references to internal security, in recitals (6) and (15), and recital (5) says that “[t]he objectives of this Directive are, *inter alia*, to ensure security.”⁴⁴⁵ Nevertheless, it is clear that the intra-EU PNR greatly interferes with the national security responsibilities of member states, starting with the purposes for which data are processed.⁴⁴⁶ A list of envisaged offenses is present in its Annex II and most headings relate to very serious crimes, as indicated above.

If doubts remained, the recent case law of the Court manages to dismiss them. In light of the fact the CJEU considered that the sole responsibility of the member states enshrined in Article 4(2) TEU “corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities...such as terrorist activities”⁴⁴⁷ and that “PNR data collected in accordance with [Directive (EU) 2016/681] may be processed only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences,”⁴⁴⁸ it seems clear that PNR systems indeed interfere with the national security agendas of the member states and fall within the scope of Article 4(2) TEU, *in fine*.

Beyond that, it should be recalled that national security operations are undertaken not only by special agents but also by law enforcement units. Under PNR arrangements, data are collected by carriers and then sent to member states’ authorities designated to act as PIUs.⁴⁴⁹ They can then transfer data to other local authorities for further examination, or appropriate action.⁴⁵⁰ Entities with access rights are chosen by the member states⁴⁵¹ and they range from

⁴⁴⁵ Recital (5) of Directive (EU) 2016/681.

⁴⁴⁶ Article 1(2) of Directive (EU) 2016/681.

⁴⁴⁷ Cases C-623/17, paragraph 74, and C-511/18, C-512/18 and C-520/18, paragraph 135.

⁴⁴⁸ Article 1(2) of Directive (EU) 2016/681.

⁴⁴⁹ Article 4(1) of Directive (EU) 2016/681.

⁴⁵⁰ Article 7(1) of Directive (EU) 2016/681.

⁴⁵¹ Article 7(3) of Directive (EU) 2016/681.

federal police bureaus to border agencies, regional and local police forces, governmental departments and ministries, intelligence agencies, military bodies, courts of law, and even fiscal authorities.⁴⁵² This proves that the Directive is well within the scope of Article 4(2) TEU, *in fine*, and the concept of national security.

The EU was competent to enact a PNR system at European level. There is no question about this. PNR falls within the scope of EU law. Yet, it also falls within the scope of the ‘sole responsibility’ of each member state. Therefore, what is questioned is how extensively the EU drew up the details of the system. The legislator should have abstained from passing such a broad, intrusive, and comprehensive scheme. This scheme left member states with very little margin to legislate and to decide on how they wanted to implement a sophisticated mechanism for the retention of personal data, which is unprecedented in EU law. It overlooked the fact that the Directive should serve only to regulate cooperation and harmonize procedures. The way it is written, the PNR Directive does not respect the diversity of national legal systems and disregards their constitutional distinctiveness.⁴⁵³

Article 4(2) appears to have two effects. For one thing, if member states have the responsibility to decide on their national security agendas and policies, and since the PNR Directive is such an intrusive piece of legislation, the adoption of a national PNR scheme should be optional. For another, there are important features of the system that could be regulated more significantly by the member states.

In the first place, PNR should be an optional security policy. Cristina Casagran has used Directive (EU) 2016/680 to show there is no need for a uniform regime on data handling by law enforcement to achieve the security goals of the Union. In fact, even with a single PNR system, passengers continue to have their personal data subject to many different processing schemes and data protection criteria, as that Directive gives a wide margin of discretion to the authorities of the member states to manage and store data once they are sent by the PIUs.

This is because the PNR Directive does not set common processing protocols for competent authorities other than the PIUs. Curiously, Directive (EU) 2016/680 leaves national legislators to decide on the implementation of protocols. As such:

If we consider this same scenario for a potential decentralised PNR regime within the EU, then each Member State would have competence to decide on the data protection rules and standards for its PNR system. Twenty-eight data protection regimes could thus potentially coexist, aside from any common EU data protection

⁴⁵² Notice (OJ C 194, 6.6.2018).

⁴⁵³ Garben, 2015: 58.

framework, and with 108 CoE Convention as solely common supranational framework.⁴⁵⁴

There are other cases in which the EU has left a margin of discretion to member states. Article 27(1) of Directive 2004/38/EC, for instance, allows them to restrict the freedoms of movement and residence of EU citizens and their families for security reasons. There is leeway for member states here and EU secondary law struck the right balance in the allocation of shared powers, while compliance with fundamental rights and EU law principles remains under Union control since its number 2 determines that any decision taken by the member states must be proportionate and based solely on individual behavior.⁴⁵⁵ This could be adapted to PNR.

To make it optional would also be in line with the aspirations of commentators following the adoption of the Treaty of Lisbon. Mitsilegas, for example, wrote, in 2010, that:

[N]ational parliaments...may obtain post Lisbon an increasingly prominent role in scrutinising proposals for EU legislation from a subsidiarity perspective. This scrutiny is particularly relevant as regards proposals related to the area of freedom, security and justice and EU criminal law in particular, where national parliaments can be informed by an agenda of preserving national autonomy with regard to decision-making and safeguarding the integrity of their domestic legal system.⁴⁵⁶

This is far from having been achieved. The treaties embrace a cooperative, and rather unique, approach in the AFSJ that the EU institutions have, to an extent, overlooked. However, the proximity of security and sovereignty favors a conservative approach in terms of having the Union meddle with substantive criminal matters. This should be viewed as a last resort, under stringent limitations.⁴⁵⁷

In the second place, the Directive should not be as intrusive as it currently is. Many features of the system should have been left for the member states to regulate, or regulate more extensively. The following examples show this clearly, referring to norms that should be purged, or rewritten, to allow national legislators to exercise responsibility. Greater attention to PNR and conferral may, one day, reveal further examples.

Article 4, on the PIUs, for instance, did not need to address how they should be staffed, or how member states have to organize themselves. It should be limited to stating that each

⁴⁵⁴ Casagran, 2015: 249.

⁴⁵⁵ Article 27(2) of Directive 2004/38/EC.

⁴⁵⁶ Mitsilegas, 2010: 466.

⁴⁵⁷ Öberg, 2017: 130.

member state needs to establish, or designate, an authority to process data and to act as liaison, similarly to how the responsibilities of the DPOs are defined in Article 5.

The processing of information, foreseen in Article 6, should also have been left for the member states to elaborate. The Union should have been concerned with limiting it in line with the purposes of the Directive, data protection laws, and fundamental rights. The EU should not have outlined how the assessment of air passengers is to take place. That should be up to national competent authorities to decide. In fact, ordering the PIUs to compare data against relevant databases,⁴⁵⁸ to process them “against pre-determined criteria,”⁴⁵⁹ or to analyze the information “for the purpose of updating or creating new [assessment] criteria”⁴⁶⁰ are unnecessary, and unnecessarily burdensome, legal requests.

Saying that processing should be non-discriminatory,⁴⁶¹ positive matches must be examined by non-automatic means,⁴⁶² DPOs need to be able to access all data,⁴⁶³ or that data must be stored in secure locations⁴⁶⁴ is, in contrast, clearly within the logic of shared competences in the AFSJ, has a connection to the legal bases (including the missing Article 16 TFEU), and respects the responsibilities of member states in national security. This would have been enough to guarantee that EU primary law, and the purposes of the security Union, are respected while national authorities gather and process PNR data.

Even the provisions on cooperation contain elements that should be for the member states to decide. Article 9 says that the exchange of data among them “may take place using any existing channels for cooperation between the competent authorities. [Plus, the] language used for the request and the exchange of information shall be the one applicable to the channel used.”⁴⁶⁵ Although relatively innocuous on first sight, these demands do not fit the logic of directives, namely being compulsory in terms of the outcomes, while allowing member states to choose the means and methods.⁴⁶⁶ Only the second part of Article 9(5) fits this logic, as it says that “Member States shall, when giving their notifications...inform the Commission of the details of the contact points to which requests may be sent in cases of emergency. The Commission shall communicate such details to the Member States.”⁴⁶⁷

⁴⁵⁸ Article 6(3)(a) of Directive (EU) 2016/681.

⁴⁵⁹ Article 6(3)(b) of Directive (EU) 2016/681.

⁴⁶⁰ Article 6(2)(c) of Directive (EU) 2016/681.

⁴⁶¹ Article 6(4) of Directive (EU) 2016/681.

⁴⁶² Article 6(5) of Directive (EU) 2016/681.

⁴⁶³ Article 6(7) of Directive (EU) 2016/681.

⁴⁶⁴ Article 6(8) of Directive (EU) 2016/681.

⁴⁶⁵ Article 9(5) of Directive (EU) 2016/681.

⁴⁶⁶ Mitsilegas, 2010: 460.

⁴⁶⁷ Article 9(5) of Directive (EU) 2016/681.

Article 14 is likewise controversial. It tables the penalties for infringements of national laws transposing the Directive, and the EU has focused on financial sanctions to carriers. Yet, how can this be framed within the purpose of cooperation? It is another example of where the Union should have remained silent and given member states space to breathe.

The PNR Directive is a necessary instrument for the pre-emptive security of the Union and of member states. Nevertheless, it is a piece of legislation that tables a system which aggressively interferes with the private life and personal data of millions of EU citizens and third country nationals. This is a sufficient basis to argue that it should, therefore, be carefully based on treaty law and be limited to the legislative powers of the Union in the AFSJ. As things stand, however, the intra-EU PNR goes beyond its treaty law bases, and the data protection norms it foresees are not built upon the treaties. On top of that, Article 4(2) TEU, *in fine*, contains a national security exception that obliges the Union to be less intrusive vis-a-vis the national security agendas and policies of the member states, leaving them with a margin of discretion to decide on such matters. The EU legislator, nonetheless, disregarded the full strength of this provision when it enacted this Directive. It is, perhaps, time for the CJEU to further explore Article 4 TEU.

Chapter 3.1

Trumping fundamental rights: Departure

“«We need to be operating at the level of Google», said Joe Leader, chief executive of the Airline Passenger Experience Association, in a report ahead of this year’s Aviation Festival.

«For every passenger, we know every detail that serves as a marketing treasure trove of personalisation. We have full names, address, exact birthdays, seat assignments, credit cards and everything that should make personalisation easy», he added. According to researchers at the Amrita School of Engineering in India, the average transatlantic flight generates about 1,000 gigabytes of data, the equivalent of about 2,000 hours of CD-quality recording.”⁴⁶⁸

Introduction

This second thematic chapter unveils the incompatibility of the PNR Directive with the rules on fundamental rights enshrined in the primary law of the EU. It is divided into three parts. This part engages with the literature, as well as the views of auxiliary and supervisory bodies and the opinions of member states and MEPs in its legislative process.

It searches for the arguments that have been tabled for and against the intra-EU PNR by academics and institutional actors. The purpose is to start exploring the viability of a possible claim that the Directive may be open to challenge on the basis that it is insufficiently protective of privacy, data protection, and other rights. Ultimately, this chapter argues that it should be declared invalid by the CJEU for violating the CFREU.

The Court tends to declare legal acts invalid, even when only certain provisions are unlawful. This was the case in joined cases C-293/12 and C-594/12 and Opinion 1/15, the two decisions that will be assessed in detail in the following part of this chapter. Although only some provisions of Directive (EU) 2016/681 appear to violate the CFREU, it is likely that the judges would also declare it entirely invalid if its validity was challenged in a preliminary ruling.

This first part is divided into two sections. The first reviews the literature on PNR and fundamental rights. This is the most heated topic discussed in relation to PNR. Yet, this section presents a more systematic review of the literature than has been available to date. It will assist readers in identifying and organizing the large body of literature that, to some degree, engages critically with PNR. This section is likewise essential to highlight the key questions which potentially make the Directive susceptible to invalidation, but need a deeper engagement. Key issues arising relate to the length of the data retention period, the data protection guarantees that

⁴⁶⁸ Hodgson & Waldmeir, 2018.

ensure the anonymity and safety of the data, especially those of a sensitive nature, access rights by third parties to PNR receipts and their content, and individual notification procedures. These issues will be explored in detail to provide the basis for the structure and content of the legal analysis in the final part of this chapter.

The second section looks at the legislative process that led to the approval of the Directive. It explores the concerns voiced by member states, MEPs, and assisting bodies. These opinions have been largely ignored in PNR studies, but they may prove relevant to understanding the broader picture of how fundamental rights have been treated. No previous study has analyzed the PNR system so comprehensively. The literature review and the analysis of these debates will help to define the scope of the legal analysis in the thesis. This chapter will identify key points of controversy, the safeguards which, authors claim, mitigate potential shortcomings in the Directive, and major recommendations for improvement tabled by the intervening parties.

The literature discussing the previous draft of the Directive has not been included. The 2011 and 2016 versions are alike and raise similar concerns. Going through the discussions on the previous proposal would be redundant. Moreover, it is not relevant for this chapter as it was rejected in 2013. Also, while most authors have looked at that version, or at the agreements between third countries and the Union, there is still work to be done regarding the adopted version of the Directive, partly because its approval coincided with that of the GDPR, which has tended to garner more attention.

This is also the reason that this chapter is limited to the institutional opinions mentioned in the Directive, or in the legislative process. Still, the EP did not ask for new opinions, in 2016, from the EDPS, the European Economic and Social Committee (EESC), or national parliaments. In those cases, the documents used are those mentioned in the legislative procedure, even if they refer to the 2011 proposal. This is without prejudice to the criticism that this is not an adequate way to legislate, especially regarding security policies that can encroach to a significant extent upon fundamental rights.

1. Reviewing the literature

The main themes addressed by the literature on PNR and fundamental rights are the tension and trade-off between public security and the rights to privacy and to data protection; the controversy concerning how modern profiling techniques used in PNR systems may lead to unlawful profiling and negative discrimination; and the transparency of the Directive in terms of notification procedures and individual data rights. These topics often surface in policy

discussions on the AFSJ. They are “révélateur des évolutions à l’oeuvre dans le champ de la sécurité intérieure européenne.”⁴⁶⁹

A basic problem in the literature is that PNR is usually criticized with vague and superficial comments. Its complicated nuances are seldom explored, many arguments are thin, and most authors do not table serious alternative proposals. Purely descriptive accounts of its functioning will not be included. This section looks, instead, at works that discuss and engage with the issues arising in relation to PNR.

An expression used by Emmanuelle Saulnier-Cassia may be revealing. He wrote that the Directive seems to be comprehensive and complete, dealing with all details in an adequate and sufficient manner. Yet, this conceals lacunae and shortcomings. Some literature on PNR is just like that. It gives an impression of thorough assessment frequently based on repeating the legislation. It does not go into the details, nor does it question the system in practice. Despite a growing literature,⁴⁷⁰ many works still deal with PNR too rapidly, and without a systematic approach or sufficient depth. Few engage with the possibility that it is “une usine à gaz des risques supplémentaires pour la protection des droits fondamentaux des individus.”⁴⁷¹

1.1 Security, privacy, and data protection

Most scholars sense PNR is at a crossroads between security policies and the fundamental rights to privacy and data protection. Noor Huijboom and Gabriela Bodea recall that, until the 9/11 terrorist attacks, European authors were concerned with preventing technologies from intruding on private lives. Then, suddenly, security and privacy were reconsidered and reshaped.⁴⁷² Their relationship has since been described as a “trade-off.”⁴⁷³

This is one of the key points of controversy that is present in almost every work on PNR. It was a divisive matter also in the legislative debates, and it underlies the reports and contributions of auxiliary and supervisory entities that will be analyzed below. To find a sustainable balance between calls for security and respecting fundamental rights is a struggle for every policy and legal act enacted in the AFSJ. PNR is no exception.

⁴⁶⁹ Bellanova & Duez, 2013: 56.

⁴⁷⁰ Bellanova, 2014: 113.

⁴⁷¹ Saulnier-Cassia, 2017: 210.

⁴⁷² Huijboom & Bodea, 2015: 242.

⁴⁷³ See, in general, Chandler, 2009.

1.1.1 Tension and trade-off

For Kerianne Wilson, API and PNR are policies that illustrate how the relationship between privacy, data protection, and security has been reframed.⁴⁷⁴ Francesca Di Matteo believes this is a delicate subject as legislators are, nowadays, called to regularly adjust the balance between the growing demands of security and the need to respect fundamental rights. In Europe, privacy has traditionally been protected by high legal standards, but security is gaining ground in governance, the media, and public opinion. PNR was born in this context of tension.⁴⁷⁵ A tension that, for Chang-Ryung Han, Rachel McGauran, and Hans Nelen, arises because one of the aims of security governance is to transform personal data into a resource.⁴⁷⁶

Some authors claim that the Directive has sufficient guarantees to protect rights, despite its security purposes. Others say these rights have been sacrificed for a vague sense of security. Others, still, believe it should include more safeguards, but still accept it as a necessary tool.⁴⁷⁷ The first group of authors analyzed here argues that PNR is satisfactory as it stands, while the second pleads for additional guarantees. Curiously, almost no one considers this tension to be about clashing rights. Despite being enshrined in Article 6 CFREU,⁴⁷⁸ security is usually perceived as a public policy, and not as a right that can be balanced, *per se*, against privacy (Article 7),⁴⁷⁹ or data protection (Article 8).

It is still not possible to identify major theoretical trends based on the current literature. The classic literature reviews in which authors are grouped around a fundamental concept cannot yet be applied to the debates on PNR, for two reasons. For one thing, they are still incipient, with few authors looking at other works. This chapter brings some added value from this perspective, as it tries to present research in a dialogue. For another, authors tend to engage with PNR in a pragmatic way. They locate a certain feature and discuss it. The more developed theoretical discussions address the tension and trade-off between fundamental rights and security. Yet, seldom do authors discuss the concept of security, for instance, or the implications of PNR for the future of fundamental rights. The latter will be better examined in the concluding remarks of this thesis, as PNR may represent a turning point in how far privacy and data protection can be curtailed in favor of security.

⁴⁷⁴ Wilson, 2016: 263.

⁴⁷⁵ Di Matteo, 2017: 213.

⁴⁷⁶ Han, et al., 2016: 1056.

⁴⁷⁷ For instance, Casagran, 2015: 257.

⁴⁷⁸ Which reads that “[e]veryone has the right to liberty and security of person.”

⁴⁷⁹ It says that “[e]veryone has the right to respect for his or her private and family life, home and communications.”

1.1.2 A necessary tool

Susanna Villani has strongly criticized PNR, but she believes it to be essential for police and law enforcement to have access to such data. She sees it as a part of the AFSJ that will make the Union safer for citizens. This should compensate for its flaws, although she does not say exactly how. She also believes that the timing of its entry into force, alongside the GDPR, is a sign that PNR adequately balances the need to protect citizens from security threats and the encroachments on fundamental rights that might occur.⁴⁸⁰ Still, Villani does not explore this, or the compensatory remedies she claims are present in the Directive.

Those claiming that the EU PNR strikes the right balance between security and rights tend to table three main arguments. Firstly, they say that only through a common instrument at Union level is it possible to arrive at that balance. In second place, they believe the Directive is imbued with sufficient data protection safeguards. And, finally, they accept the long data retention period, as they find it necessary to facilitate the conduct of complex criminal investigations.

A. Common instruments for EU security

Villani argues that harmonization through a Directive is preferable to leaving member states to regulate PNR autonomously. She believes that this is because local parliaments may give in to a certain security appeal and thereby fail to protect privacy.⁴⁸¹ Harmonized legislation at EU level is, indeed, more likely to foresee common guarantees to shield fundamental rights.

This is a relevant takeaway. Regardless of the flaws of the intra-EU PNR system, to have a single instrument guiding the legislation of the member states is preferable in many regards, especially to protect fundamental rights. Villani's opinion is shared by Elena Carpanelli and Nicole Lazzerini, as well as Francesca Di Matteo.⁴⁸² The privacy guarantees they identify in the Directive, which could be missing if PNR were left entirely in the hands of the member states, are the establishment of PIUs, mandatory supervision by entities at Union and national level, specifically DPOs, and the use of the push method.

⁴⁸⁰ Villani, 2018: 926.

⁴⁸¹ *Idem*: 902.

⁴⁸² Carpanelli & Lazzerini, 2017: 395, and Di Matteo, 2017: 231.

Likewise, Bogdan Bîrzu⁴⁸³ and David Lowe⁴⁸⁴ claim that PNR is an adequate and necessary tool for European security. Villani would later reinforce this, saying that it is consistent with other such data security practices, as well as the aim of law enforcement collaboration.⁴⁸⁵ These opinions echo that of Cristina Casagran, who had previously argued that PNR systems offer robust, reliable, and appropriate data protection tools, suitable for the EU's internal market.⁴⁸⁶

The idea of PNR being necessary for EU security is reiterated by Han, McGauran, and Nelen. Albeit stressing that it collects so much data from air passengers that it can lead to a permanent trace on their whereabouts, they believe it to be an indispensable measure.⁴⁸⁷ Borrowing the idea from Kerianne Wilson, they argue that the intangible opportunity cost of revealing passengers' information (in other words, interfering with their privacy), is a necessary price to pay for keeping people safe.⁴⁸⁸

The security appeal is such a strong argument that it even influences authors known for criticizing PNR. Andrea Chiappetta and Andrea Battaglia, for example, though recognizing that it is a disruptive tool, claim that its weight in fighting terrorism is vital.⁴⁸⁹

B. Mechanisms of data protection

Han, McGauran, and Nelen have applied a privacy test developed by Adam Moore⁴⁹⁰ to PNR. They concluded that these data are not as confidential as telephone calls or e-mails since they have always been available to air carriers and non-carrier operators. Besides, despite data being gathered mostly for purposes unrelated to security, passengers know and expect that border authorities will access and monitor their movements on a regular basis.⁴⁹¹ The risk to privacy does not appear excessive, since the Directive excludes the need for courts to authorize access to data by law enforcement. In their view, if the interferences were excessive, the Directive would have included such procedures.

However, the final text does include prior review mechanisms. This is a good example of what is often missing in the legal analysis of key issues undertaken by scholars until now.

⁴⁸³ Bîrzu, 2016: 205. This author makes interesting proposals *de lege ferenda* to improve the Directive. Most, if not all, have been added to the final text.

⁴⁸⁴ In general, Lowe, 2016.

⁴⁸⁵ Villani, 2018: 915.

⁴⁸⁶ Casagran, 2015: 257.

⁴⁸⁷ Han, et al., 2016: 1056.

⁴⁸⁸ *Idem*: 1059.

⁴⁸⁹ Chiappetta & Battaglia, 2018: 78.

⁴⁹⁰ Moore, 2011.

⁴⁹¹ Han, et al., 2016: 1058 and 1059.

Authors have often failed to study carefully the final version of the EU PNR. In fact, while the 2011 proposal did not require that access to depersonalized data be dependent on the approval of a judicial authority, Directive (EU) 2016/681 does, in Article 12(3)(b), point i. It is a safeguard that helps to justify its adoption, but which will be revisited in the final part of the chapter, since it has important limitations to consider. Contrary to what Han, McGauran, and Nelen argued, courts do need to authorize access to data in many situations. Does this mean that the risks to privacy are excessive after all?

Certain scholars believe that cautious attitudes towards the collection of big data are a sort of paranoia. Arthur Rizer, for example, considers it to be a reaction to recollections of Nazi and Soviet control.⁴⁹² David Lowe finds that the debates on balancing security and fundamental rights have been one of the primary impediments to achieving fruitful negotiations and adopting an internal system. They apparently stem from “fear of expanding a surveillance society.”⁴⁹³ Lowe adds that this fear might have been understandable regarding the external agreements and the 2011 proposal, but it is ill-founded *à propos* the 2016 Directive, which is brimming with data protection tools.⁴⁹⁴ Still, he fails to identify them, thus weakening his argument.

This author concludes that the Directive is fit for purpose, because it manages to protect personal data. This is based on features like the need to appoint DPOs to work at the PIUs to monitor data processing operations and apply appropriate precautions.⁴⁹⁵ Plus, as DPOs are the single contact points for data subjects, this seems to suffice in ensuring privacy, as all matters are dealt with in a centralized and controlled manner.⁴⁹⁶ This is reinforced by the fact that its Article 6(8) obliges the PIUs to process and store data in safe places. These are good points and relevant improvements. Yet, these features make the protection of the information dependent on the performance of external entities. They do not stem directly from obligations embedded in the system, developed as security-by-design technology.

Lowe also judges the guarantees on data transfers to be adequate. He argues that Article 11, on transfers with third countries, read together with Article 13, on the protection of data, lay out a set of sufficient conditions for the exchange of data outside the Union. Given that third countries must provide an adequate level of protection, and DPOs must be informed of every transfer, this author believes that compliance with European data protection laws and the rulings

⁴⁹² Which, for the author, is what explains the different views towards law enforcement collecting personal data in Europe and in the US (Rizer, 2010: 78).

⁴⁹³ Lowe, 2016: 858 and 869.

⁴⁹⁴ *Idem*: 881.

⁴⁹⁵ Article 5(1) of Directive (EU) 2016/681.

⁴⁹⁶ Lowe, 2016: 875. See Article 5(3) of Directive (EU) 2016/681.

of the CJEU has been achieved. Oddly, it is not clear which legal instruments, or case law, he has in mind. Plus, this argument will be unpacked and deconstructed in chapter 3.3, as Article 11 is not watertight, presenting holes that third countries can exploit to collect data from EU citizens without guaranteeing an adequate level of protection at all times.

Enrique Pérez-Luño Roledo likewise considers the Directive to offer general guarantees to keep data safe.⁴⁹⁷ This is based on the fact that member states are required to ensure that their PIUs offer enough technical measures to maintain adequate levels of security.⁴⁹⁸ Villani had previously voiced a similar view,⁴⁹⁹ stressing that the use of sensitive data is prohibited and that the push method⁵⁰⁰ prevents member states from accessing carriers' files.⁵⁰¹

C. Data retention period

While Susanna Villani and Giulia Tiberi contend that five years is an overly long period which leaves data unnecessarily exposed,⁵⁰² Bîrzu defends the opposite position. He maintains that the Directive is sufficiently limited, since data are not retained for more than a fixed period of five years and are masked six months after collection.⁵⁰³ Still, he fails to explore precisely why data are left unmasked during these initial months, and the effects this may have on their safety. This is an aspect that few authors scrutinize, despite the impact that faulty depersonalization mechanisms can have on the overall safety of data and, therefore, on the privacy of air passengers. It will be an important feature of the final legal analysis, even though it has, so far, been little more than a marginal note.

Pérez-Luño Roledo adheres to this view, stressing that the right to be forgotten is guaranteed in all processing operations. He believes that Article 12, on the retention of data and depersonalization, is adequate when judged by the standards of Article 17 of GDPR, on the right to be forgotten.⁵⁰⁴ He repeats the depersonalization argument, highlighting the apparently strict access conditions.⁵⁰⁵ Yet, it remains unclear what problems derive from having data

⁴⁹⁷ Pérez-Luño Robledo, 2019: 234.

⁴⁹⁸ See Article 13(7) of Directive (EU) 2016/681.

⁴⁹⁹ Villani, 2018: 913.

⁵⁰⁰ See chapter 1 for a definition of this method, in contrast with the pull method.

⁵⁰¹ Articles 3, paragraph 7, and 8 of Directive (EU) 2016/681. See also recital (16).

⁵⁰² Villani, 2018: 917, and Tiberi, 2016: 592.

⁵⁰³ Bîrzu, 2016: 196.

⁵⁰⁴ This has become a common expression after the ruling of the CJEU in case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 13 May 2014 (ECLI:EU:C:2014:317). However, it has no legal value, especially considering it is part of the title of the provision and not of its normative content. It reads “[r]ight to erasure (‘right to be forgotten’).”

⁵⁰⁵ Articles 12(2) and (3) of Directive (EU) 2016/681. Pérez-Luño Robledo, 2019: 234 and 235.

retained for long periods of time, whether masking up is sufficient as it stands, or how potential difficulties can be overcome. Again, despite its insufficiencies, existing literature proves to be crucial in identifying key points of debate.

1.1.3 Insufficient guarantees

Other authors have called for additional guarantees to protect the privacy and the integrity of data of passengers in the intra-EU PNR. Brendan Lord says that pro-privacy authors have detected several issues with the functioning of the system, most related to the quantity of collected data and potentially unlawful profiling.⁵⁰⁶ Still, on the tension between security and fundamental rights, the main arguments used to challenge the Directive are its long data retention period, and its ambiguity regarding the authorities that can access PNR receipts.

A. Data retention period

The deficiencies of the Directive in protecting data stem, for most authors, from the lengthy retention period. Many claim that a key improvement would be a shortening of this period. In fact, Georgios Nouskalis claimed, in 2011, that five years is a disproportionate encroachment upon privacy, in order to deflect indeterminate hazards.⁵⁰⁷ He failed to elaborate further, but Emmanuel Saulnier-Cassia has developed the idea. For him, the possibility of revealing (de-masking) passenger data for four and a half years is too easy and, therefore, too dangerous. As an *ex ante* approval by a judicial authority to access data can be replaced by that of any competent national agency,⁵⁰⁸ he believes anonymity, in PNR, “n’est donc qu’un leurre.”⁵⁰⁹

Giulia Tiberi agrees with them, stressing that PNR data are retained longer than any other data collected under security policies, even the invalidated Directive 2006/24/EC.⁵¹⁰ For Nora Loideain, a lengthy period renders the Directive less in line with fundamental rights and the case law of the CJEU.⁵¹¹ It is unfortunate that she fails to dig deeper into this idea. In any case, these are weighty arguments. The length of PNR’s data retention period is a matter that will be analyzed in depth in chapter 3.3.

⁵⁰⁶ Lord, 2019: 268. See also, Mendes de Leon, 2017: 320.

⁵⁰⁷ Nouskalis, 2011: 476.

⁵⁰⁸ Article 12(3)(b), point ii, of Directive (EU) 2016/681.

⁵⁰⁹ Saulnier-Cassia, 2017: 218.

⁵¹⁰ Its Article 6 foresaw that information could be “retained for periods of not less than six months and not more than two years from the date of the communication.”

⁵¹¹ Loideain, 2015: 59.

Tiberi also refers to an important criticism mentioned by other scholars and even the CJEU. The Directive does not provide for specific retention periods according to different categories of data.⁵¹² Yet, certain data allow for easier identification of passengers, like names or contact details. As such, some scholars argue that the retention period should be tailored according to the interference with fundamental rights of each data element. This is another crucial suggestion for improvement that will be developed in the legal analysis of chapter 3.3.

Di Matteo sides with this argument, adding that PNR disrespects the data minimization principle.⁵¹³ This principle should always guide the processing of data⁵¹⁴ as it obliges processors to reduce the amount of data they access and use.⁵¹⁵

B. Third parties with access rights

On a different level, Olga Enerstvedt argues that the Directive should not be silent on the third country authorities with access rights. Other recommendations that could improve the PNR system would be to lay down precise guidelines on processing operations undertaken outside the EU, as well as include mechanisms to ensure data protection standards are applied abroad.

These recommendations are interesting, although they could be difficult to implement. They stem from the purpose limitation principle, which also concerns transfers to third countries.⁵¹⁶ Enerstvedt sees this principle as a key tool to constrain data processing, inside and outside the Union. Unfortunately, she does not make her argument more concrete by suggesting how she would change the text of the Directive and operationalize these suggestions. She just concludes that a balance must be found between purpose limitation requirements and the correct functioning of the system.⁵¹⁷

Saulnier-Cassia has built on top of this to argue that the Directive should not allow member states to transfer data outside the EU without the consent of other member states, especially those whose nationals' data could be involved in such transfers.⁵¹⁸ Again, this seems a sensible recommendation, but it might be in tension with the need to have a speedy and efficient system.

Regarding internal transfers, Enerstvedt makes a key legal argument when criticizing Article

⁵¹² Tiberi, 2016: 592. She is here following the jurisprudence of the CJEU in joined cases C-293/12 and C-594/12, paragraph 64.

⁵¹³ Di Matteo, 2017: 232.

⁵¹⁴ Tiberi, 2016: 592 and 593.

⁵¹⁵ For further developments on this topic see Enerstvedt, 2017: 194 ff., and, in general, Gilbert, 2007.

⁵¹⁶ Enerstvedt, 2017: 355.

⁵¹⁷ *Idem*: 356.

⁵¹⁸ Saulnier-Cassia, 2017: 224 and 225.

9 for being unnecessarily confusing. This is a blatant shortcoming of the Directive that will be assessed later in the thesis. Article 9 tables a set of criteria to allow for the exchange of information, while letting member states skip the enforcement of data protection guarantees.⁵¹⁹ First, Article 9(2) allows for transfers between PIUs of unmasked data through “duly reasoned [requests and for a] specific case of prevention, detection, investigation or prosecution of terrorist offences or serious crime.”⁵²⁰ Its number 3 adds that authorities “may request directly the PIU of any other Member State to provide them with PNR data...when necessary in cases of emergency and under the conditions laid down in paragraph 2.”⁵²¹ And, finally, number 4 allows any PIU to require other PIUs for data “[e]xceptionally, where access to PNR data is necessary to respond to a specific and actual threat related to terrorist offences or serious crime.”⁵²² The redundancy of these provisions is notorious. They open too many avenues for information to circulate among member states, which can weaken legal security and certainty, while concealing the limitations of the Directive.⁵²³

1.2 Profiling and discrimination

A second common theme for discussion is the matter of profiling and how it can lead to negative discrimination. Only Timothy Kirkhope, the rapporteur of the LIBE Committee for PNR, is known to have said that no profiling occurs through use of PNR.⁵²⁴ This is a dangerous opinion. It conceals one of the most preoccupying features of the system, its ability to classify passengers in a way that human operators do not fully understand, but on the basis of which they must take relevant decisions, including those relating to the possible detention of persons.

Profiling occurs in PNR systems. There is a consensus about this in the literature. What has divided scholars is whether the Directive’s profiling system is a necessary and acceptable price to pay. A minority faction thinks that the efficiency of PNR depends on profiling and accepts it as it is, while a large majority of authors considers that it should be reviewed. They fear that this system will eventually lead to negative discrimination and incorrect predictive assessments based on a black box of impenetrable algorithms, whereby human agency is rendered a remote feature of the final decision-taking.

⁵¹⁹ Enerstvedt, 2017: 354.

⁵²⁰ Article 9(2) of Directive (EU) 2016/681.

⁵²¹ Article 9(3) of Directive (EU) 2016/681.

⁵²² Article 9(4) of Directive (EU) 2016/681.

⁵²³ Enerstvedt, 2017: 354.

⁵²⁴ Intervention by Timothy Kirkhope on the debate on the Use of Passenger Name Record data (EU PNR), sitting of the European Parliament of 13 April 2016.

The following sections will unpack the arguments regarding profiling and negative discrimination. First, however, it is important to explain how scholars perceive profiling in the intra-EU PNR system.

1.2.1 Modern profiling techniques

Profiling is the process⁵²⁵ of classifying and treating people according to pre-determined criteria.⁵²⁶ Ben Wagner explains that this usually happens with machines processing data by means of algorithms that suggest whether a person is statistically likely to be a criminal or to belong to a criminal network.⁵²⁷ They then supply that data to law enforcement to check whether these matches are correct.

The PNR Directive carefully avoids using the term profiling, or related words. This is, perhaps, a way to lessen the impact that such vocabulary could have if it was openly used in this piece of legislation. However, the processing undertaken by the PIUs and other law enforcement authorities necessarily leads to the profiling of air passengers. The key issues arising are, in fact, how people are sorted through and whether profiling operations lead to positive or negative discrimination, i.e., segregation based on prohibited criteria.

PNR data can be sent to the PIUs before take-off, which enables law enforcement to ask for such information before, or immediately upon arrival. Profiling is mostly done automatically. Wagner adds that PNR is often coupled with data from social media to augment what national authorities know about passengers. This is made easier as most passengers log in to their accounts on Global Distribution Systems through social media.

New technologies have transformed profiling, allowing for instant processing that boxes people into groups based on risk analysis. Already in 2011, Paul De Hert and Rocco Bellanova suspected that modern technologies, like the ones used to profile passengers in PNR systems, could give rise to problems with fundamental rights, as well as in terms of “non-discrimination, presumption of innocence, and due process.”⁵²⁸ Matthias Leese recalls that the degree of risk to fundamental rights in data-based profiling (also called preventive analytics) is higher than in standard criminal investigations. With big data, it becomes easier and faster to connect the dots

⁵²⁵ Either automated, manual, or involving both human and machine elements.

⁵²⁶ Enerstvedt, 2017: 285.

⁵²⁷ Wagner, 2019: 110.

⁵²⁸ De Hert & Bellanova, 2011: 491.

and get added value from data that were apparently irrelevant when seen independently.⁵²⁹ Yet, the risk of intrusion and of committing errors is also higher.

1.2.2 A necessary tool

A few authors consider that profiling in PNR is necessary, or even acceptable. Enerstvedt believes that only through targeted profiling of air passengers can PNR be efficient.⁵³⁰ She and Steve Wolff agree that, without profiling techniques, “clean-skin”⁵³¹ terrorists could pass security checks unnoticed.

On the other hand, Enerstvedt acknowledges that negative discrimination can also take place.⁵³² She and Bart Schermer suggest that the efficiency of data mining might decrease if sensitive data are prevented from being used in the system. They fear that this could increase false results. However, while Schermer backs up this position and admits that it is preferable to sacrifice efficiency rather than privacy, advocating for security systems that are designed to be especially attentive to discrimination,⁵³³ Enerstvedt is silent in this regard.⁵³⁴ She admits that the use of sensitive material does appear to breach the principle of equality⁵³⁵ but it is not clear whether she is against the discrimination possibly occurring in PNR schemes.

1.2.3 Unlawful profiling and discrimination

Most academic work accepts, to different degrees, that using PNR segregates people in an unlawful way. Still, there is no main argument and, unfortunately, some scholars do not explain exactly the manner in which this profiling occurs in the EU system. In any case, the fact that it allows for the use of sensitive data to discriminate is the key takeaway from this literature. It is a feature that will be more fully explored in the legal analysis.

⁵²⁹ Leese, 2014: 501 and 502.

⁵³⁰ Enerstvedt, 2017: 274.

⁵³¹ Wolff, 2012: 5.

⁵³² The author distinguishes between direct and indirect discrimination. The former takes place by means of using sensitive data, while the latter depends on the use of non-sensitive data, that is, neutral data (Enerstvedt, 2017: 304). She explains the concept of neutral data with an example recurrent in the literature. It has happened that certain individuals have been submitted to physical searches, or barred from flying, only because their names were similar to those of known terrorists and criminal offenders. One’s name is an example of neutral data.

⁵³³ Schermer, 2011: 51.

⁵³⁴ Enerstvedt, 2017: 289.

⁵³⁵ *Idem*: 290.

Matthias Leese claims that the more data are collected, the higher is the chance of finding patterns that can be used in meaningful ways.⁵³⁶ This has been standard procedure in commerce for a long time, primarily to increase sales based on consumer behavior.⁵³⁷ This is, in a way, also the logic behind PNR. Yet, while algorithmic operations used in business are usually innocuous and serve limited commercial purposes, Leese alerts us to the risks of profiling applied to security, namely those stemming from incorrect predictive assessments⁵³⁸ and operational errors.

A. Operational errors and incorrect predictive assessments

Paul De Hert and Rocco Bellanova have taken a close look at operational errors. They believe the literature on PNR should be more attentive to these particular failures of the system.⁵³⁹ Classic criminal investigations depend on reasonable suspicion, or a similar level of certainty, to persuade the judiciary into issuing search warrants or detention orders. Yet, this does not happen with PNR systems. Law enforcement authorities must submit a reasoned request to access data from the PIUs.⁵⁴⁰ However, the Directive does not require them to have a high level of suspicion resulting from an ongoing investigation targeting concrete individuals each time they require data from any given flight.

A low suspicion threshold, especially if access is not necessarily authorized by courts or independent authorities, amplifies the chances and consequences of errors. One of the operational errors identified by De Hert and Bellanova could have a serious discriminatory effect. It was already present in the 2011 proposal⁵⁴¹ and was not corrected in 2016. Carriers can add “general remarks”⁵⁴² to PNR receipts that will help provide personalized services to air passengers. The issue is that the Directive allows for such remarks, which can contain sensitive data, to be sent to the PIUs and be disclosed alongside the other data in the PNR receipts.

There are many problems with this opening of the system, starting with its open-ended nature and broad potential access to sensitive material. Plus, these remarks can often be incorrect or misrepresentative, thus making passengers a sitting duck for inaccurate assessments. This key

⁵³⁶ Leese, 2014: 501 and 502.

⁵³⁷ See, in general, the adaptation of this behavioral analysis to preemptive security by Rouvroy, 2013.

⁵³⁸ A broad study on using data mining for predicting crime and analyzing intelligence in different scenarios can be found in McCue, 2015.

⁵³⁹ De Hert & Bellanova, 2011: 495.

⁵⁴⁰ Articles 6(2)(b) and 9(3) of Directive (EU) 2016/681.

⁵⁴¹ Item (12) of Annex I of Proposal for a Directive (COM(2011) 32 final, 2011/0023 (COD), 2.2.2011).

⁵⁴² Item (12) of Annex I of Directive (EU) 2016/681.

issue is going to be explored in depth later in this chapter. It is a shortcoming that could easily have been avoided, especially considering that it has been identified for quite some time. The authors conclude that the legislator should protect passengers from such errors. And it “goes without saying that the added value of this «guess work» has [yet] to be solidly proven.”⁵⁴³

Such openings and errors in processing can lead to incorrect predictive assessments, which can become a serious problem due to the use of modern technologies that process data at an unprecedented scale and speed. Mathias Leese thinks that, as decision-making in security procedures is systematically pressured by time limitations,⁵⁴⁴ adding speed to the unpredictability of algorithmic results, and the general suspicion that pervades security operations, may easily lead to biased social sorting.

Already during the discussions on the first PNR proposal, some authors feared that the preventive uses of data “introduiraient *de facto* un système de *data mining* et de *profiling* à échelle européenne.”⁵⁴⁵ Paul De Hert and Vagelis Papakonstantinou would later reaffirm this, saying that profiling is the elephant in the room in PNR. And the problem is that all versions of PNR are based on opaque preemptive assessments.

They are based on “une approche inductive [instead of] une approche hypothético-déductive.”⁵⁴⁶ De Hert and Papakonstantinou argue that, in a way, this makes data mining operations highly mistrustful.⁵⁴⁷ In the words of Antoinette Rouvroy and Thomas Berns, with a deductive approach, data are verified against databases to confirm what is already suspicious. With an inductive approach, on the other hand, law enforcement tries to make discoveries, i.e., to access and link unknown facts.⁵⁴⁸ This is what happens with the use of PNR. The issue is that, while some of these discoveries may reveal unknown criminals, many operations target innocent individuals, turning them into suspects with little respect for their freedom of movement, privacy, or the integrity and secrecy of their data.

B. Negative discrimination

Such biased social sorting may give rise to unlawful discrimination against certain categories of passengers. Didier Bigo and other authors have contended that the risk criteria used to profile

⁵⁴³ De Hert & Bellanova, 2011: 495.

⁵⁴⁴ Leese, 2014: 502.

⁵⁴⁵ Bellanova & Duez, 2013: 55.

⁵⁴⁶ Idem: 56.

⁵⁴⁷ De Hert & Papakonstantinou, 2015: 163.

⁵⁴⁸ Rouvroy & Berns, 2010: 91 and 92.

passengers in PNR tend to target those with a “second (‘foreign’) nationality or foreign background [in] a *person-centric approach*.”⁵⁴⁹ They are also often based on criminally irrelevant behavior and innocuous physical traces.

Discrimination, as Schermer sees it, is an inevitable part of data mining and profiling operations.⁵⁵⁰ Toon Calders and Indre Zioblaite stress, from a different angle, that racial profiling often leads to discrimination in security checks at airports.⁵⁵¹ Yet, they also recall that security operations aim at positive and necessary discrimination. The literature tends to forget this, although it is a sound idea. Positive discrimination, or differentiation, of passengers is essential to make people safe. What is important, in security checks and in the PNR system as a whole, is that this differentiation is regulated and limited so it does not escalate into negative discrimination, i.e., that these systems do not become based on biased or irrelevant traces but remain dependent on concrete risk factors.

Suspicious profiles need to be verified by a human controller, which is a key safeguard in the Directive.⁵⁵² Plus, there are as yet no cases of PNR data mining patterns constituting evidence in court. Despite this, Enerstvedt has insisted on the perils of negative discrimination and the impact of false positives on fundamental rights. They do not only affect privacy and data protection.⁵⁵³ False positives can lead to having innocent passengers detained, deported, added to no-fly lists, or included in watch lists.⁵⁵⁴ They can thus affect many other rights and values, from freedom of movement to human health.

The processing of sensitive material is perceived by different authors as the cause, or origin, of most disproportionate interferences with fundamental rights. Sensitive data are those that cannot serve as grounds to differentiate people, save for reasoned exceptions. Otherwise such discriminatory operations are prohibited.⁵⁵⁵

Enerstvedt emphasizes an aspect that is discussed by the CJEU in this regard. Any decision taken by law enforcement where sensitive data are relevant despite the behavior of the passengers individually considered disregards the rights enshrined in Articles 7, 8, and 21 CFREU.⁵⁵⁶ She thinks that the freedom of movement of EU citizens should be curtailed only based on individual criminal conduct and threats to security. Enerstvedt is here echoing Bigo,

⁵⁴⁹ Bigo, et al., 2015: 12.

⁵⁵⁰ Schermer, 2011: 47. Also, Enerstvedt, 2017: 304.

⁵⁵¹ Calders & Zioblaite, 2013: 47.

⁵⁵² See, for instance, Articles 7(6) or 12(5) of Directive (EU) 2016/681.

⁵⁵³ De Hert & Bellanova, 2011: 491.

⁵⁵⁴ Enerstvedt, 2017: 283 and 284.

⁵⁵⁵ Article 21 CFREU.

⁵⁵⁶ Opinion 1/15, paragraph 165.

who believes that PNR enters into direct conflict with the Schengen principles. They “prohibit systematic checks and surveillance of EU citizens on the move, which is precisely what instruments such as the EU PNR [seek] to establish.”⁵⁵⁷

In this sense, Saulnier-Cassia does not believe that Articles 6(4), 7(6), and 13(4) of Directive (EU) 2016/681⁵⁵⁸ are sufficiently watertight to prevent sensitive data from being processed and to oblige PIUs to delete them if they appear in PNR receipts. A first problem is that these norms, aimed at preventing such processing, have a more limited scope than Article 21(1) CFREU.⁵⁵⁹ A person’s color, genetic features, or even property, he says, can be assessed for the purposes of the intra-EU PNR.⁵⁶⁰ Although Bîrzu claims that the scope of the Directive expressly bans the use of sensitive data,⁵⁶¹ this is not enough to prevent possible discriminatory actions. The criticism holds and it is a key recommendation for improvement to consider in the legal analysis of chapter 3.3.

1.3 Data rights and transparency

The final theme for discussion, data rights, is an issue that makes authors engage more deeply with the Directive and the functioning of PNR. The right to notification tends to emerge in the literature as the most relevant of the various data rights. If passengers know whether, how, when, and for what purposes their data are processed, Villani states that they will be able to exercise all other rights.⁵⁶² Once again, there are authors who believe the PNR Directive contains sufficient guarantees, and there are those who disagree.

1.3.1 Sufficient guarantees

Only a few authors think the PNR system adequately protects individual data rights. Most base their claims on the Directive’s references to national supervisory authorities⁵⁶³ and to the DPOs working in the PIUs.⁵⁶⁴ Villani believes that the legislator paid attention to the ideas of the

⁵⁵⁷ Bigo, et al., 2015: 2 and 12.

⁵⁵⁸ See also recitals (15), (20), (36) and (37).

⁵⁵⁹ It reads that “[a]ny discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.”

⁵⁶⁰ Saulnier-Cassia, 2017: 217.

⁵⁶¹ Bîrzu, 2016: 196.

⁵⁶² Villani, 2018: 913.

⁵⁶³ Articles 6(7), 13(5) and (6), and 15, as well as recitals (32) and (37), of Directive (EU) 2016/681.

⁵⁶⁴ Articles 5, 6(7), 10(3), and 12(3)(b), point ii, and recital (37) of Directive (EU) 2016/681.

EDPS during the legislative process regarding the supervision of data processing.⁵⁶⁵ Lowe has made a similar argument, seeing in the supervisors a development that distinguishes the 2016 Directive from the 2011 proposal. He considers that member states are now obliged to ensure that processing is lawful and that complaints are addressed.⁵⁶⁶ He also claims that Article 15 is a crucial step in ensuring an accountable system, since it makes national supervisory bodies competent to conduct investigations and to advise member states on the enforcement of PNR.⁵⁶⁷

Villani further recalls that member states are required to keep an updated list of authorities that may request access to PNR data. As the Commission must be notified of any changes, this guarantees institutional transparency and allows passengers to know what entities are entitled to access their data.⁵⁶⁸ Although not agreeing entirely with their positions, Enerstvedt says that this can also serve the principle of purpose limitation, provided these lists are exhaustive.⁵⁶⁹

These are important remarks to take on board. The approved version of the Directive is characterized by positive developments that help mitigate its potential shortcomings with regards to transparency, and even supervision. Yet, controversy has persisted over the years, especially due to the fact that data subjects are still left in the dark regarding why and how their data are processed, as well as the reasons justifying their segregation.

1.3.2 Insufficient protection

Most scholars disagree with Lowe and Villani. Mathias Bug and Sebastian Bukow argue that passengers, even frequent flyers, are not usually aware of PNR. It is not a widely known or discussed measure, which renders it opaque and distant.⁵⁷⁰ Enerstvedt is one of the scholars

⁵⁶⁵ Villani, 2018: 914.

⁵⁶⁶ Lowe, 2016: 875.

⁵⁶⁷ Article 15 of Directive (EU) 2016/681 reads that “1. Each Member State shall provide that the national supervisory authority referred to in Article 25 of Framework Decision 2008/977/JHA is responsible for advising on and monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive. Article 25 of Framework Decision 2008/977/JHA shall apply. 2. Those national supervisory authorities shall conduct activities under paragraph 1 with a view to protecting fundamental rights in relation to the processing of personal data.”

⁵⁶⁸ Villani, 2018: 914. She was referring to two provisions of the Directive. On the one hand, Article 4(5), which says that “[w]ithin one month of the establishment of its PIU, each Member State shall notify the Commission thereof, and may modify its notification at any time. The Commission shall publish the notification and any modifications of it in the *Official Journal of the European Union*.” On the other, Article 7(1), which states that “[e]ach Member State shall adopt a list of the competent authorities entitled to request or receive PNR data or the result of processing those data from the PIU in order to examine that information further or to take appropriate action for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime.”

⁵⁶⁹ Enerstvedt, 2017: 352.

⁵⁷⁰ Bug & Bukow, 2017: 303. In their work, these authors have compared the acceptability of PNR and of the retention of communications data by German and British individuals. One of their conclusions is that PNR has been more broadly welcomed in the United Kingdom, although acknowledging that citizens in both countries are generally unfamiliar with it. This led them to argue that “new, less well-known, measures are more likely to be

who has better explored this topic, pointing to four key issues of transparency and data rights during processing operations in the PNR scheme.

The first problem is that the Directive is unclear regarding how passengers can access their PNR receipts.⁵⁷¹ Plus, if data are to flow through different databases, it may be the case that records stored in one place are outdated, or do not correspond with those held by other entities. There are no guarantees of uniformity in the Directive. To overcome this, air passengers would have to ask for their data simultaneously from all entities. As this is not feasible, there appears to be an issue of lack of transparency by design.

A second problem is closely related. Enerstvedt thinks that data controllers and processors might find it difficult to comply with requests for access from data subjects. This is because not all have implemented mechanisms enabling them to produce copies of receipts which are accessible, or readable, by the public. She illustrates this with the complications faced by MEP Sophia In't Veld to access her files from flights she took to the US, as well as a similar case experienced by Edward Hasbrouck in the Netherlands.⁵⁷² These situations are more than a decade old. Yet, they should be used as examples to press for an evaluation of notification procedures in the current system, especially considering In't Veld only managed to access her PNR after filing a lawsuit. And she was only given partial access to her own personal data.

The third issue concerns the lists of authorities with access rights. The author argues that, by not including a list of entities with access rights or, at least, by not specifying the databases against which data are run, the Directive fails to meet basic transparency requirements. Still, it is not clear how this could be improved. Leaving member states to decide who those authorities are, as is currently the case,⁵⁷³ seems the only possible scenario in light of the differences among national legal systems.

Enerstvedt's final remark flows from the previous issue. This is an aspect meriting close attention, and which will be developed in more depth in the doctrinal part of this chapter. She argues that passengers do not know which data are being processed, when, by whom, or for what reasons. This happens for two reasons.

First, the Directive is silent on whether PNR receipts must be transmitted in full, or only partially, whenever law enforcement requires them from the PIUs. This appears to be a question

accepted by those who are already familiar with widespread security measures" (305). In fact, Britain has systematically implemented more security policies than Germany. Many are openly visible to the public, like Closed-Circuit Television installations. In the authors' view, this has made the British people generally more insensitive to new security policies, like PNR.

⁵⁷¹ Enerstvedt, 2017: 386.

⁵⁷² *Idem*: 387.

⁵⁷³ Article 7 of Directive (EU) 2016/681.

left to be settled on a case-by-case basis. Yet, it may generate uncertainty.⁵⁷⁴ In second place, as mentioned regarding operational errors and incorrect predictive assessments, heading (12) of its Annex I says that carriers can include in the PNR receipts:

General remarks (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).⁵⁷⁵

Even if this is intended to apply to unaccompanied minors, it still allows carriers to add all kinds of observations to receipts, from dietary habits to health information. This increases the risk of having sensitive data circulating. Additionally, Elena Carpanelli and Nicole Lazzerini comment that heading (5), on address and contact data, is likewise problematic, because it does not identify whether these data must belong to passengers, or to them and other people involved in the flight arrangements.⁵⁷⁶

There are other scholars arguing against the lack of transparency and criticizing the way in which it may encroach upon data rights. Tarleton Gillespie joins Bug and Bukow, for instance, in saying that individuals are seldom aware of secondary uses of data when they book air tickets. PNR has been designed to operate behind a veil of opacity which makes it impermeable.⁵⁷⁷

In fact, PNR is a textbook example substantiating the fears of Mireille Hildebrant and Serge Gutwirth. Trailing the work of Frank Pasquale,⁵⁷⁸ they assert that “data mining techniques remain a technological black box for citizens.”⁵⁷⁹ Enerstvedt also puts it in an interesting way, referring to the lack of “algorithmic transparency.”⁵⁸⁰

This “loss of traceability”⁵⁸¹ makes passengers unaware of how their personal data are used, rendering them powerless to exercise their data rights. Leese contends that transparency is slowly disappearing from data retention systems. People interact with these schemes without realizing what happens to their data. Private and public entities profile individuals in invisible ways and often do not give them the tools, or opportunities, to react. Oscar Gandy stresses that

⁵⁷⁴ Enerstvedt, 2017: 314.

⁵⁷⁵ Heading (12) of Annex I of Directive (EU) 2016/681.

⁵⁷⁶ Carpanelli & Lazzerini, 2017: 393.

⁵⁷⁷ Gillespie, 2014: 192.

⁵⁷⁸ See, in general, Pasquale, 2015.

⁵⁷⁹ Hildebrant & Gutwirth, 2008: 367.

⁵⁸⁰ Enerstvedt, 2017: 314 ff.

⁵⁸¹ Leese, 2014: 504.

most passengers only know they have been profiled when they experience the offline effects, like being detained, or listed as no-flyers.⁵⁸²

This literature review has highlighted the main tensions that divide scholars in relation to the merits and hazards of PNR. The arguments that will sustain the doctrinal claim in the last part of this chapter are starting to take shape. In fact, the thesis builds on top of previous scholarly writing and takes it a step further in unpacking what is wrong, legally speaking, with the PNR Directive from the perspective of fundamental rights. And there is already a substantial set of relevant takeaways from the existing literature that will help us move forward.

A PNR system is seen by most authors as essential to keep the EU and its member states safe in light of modern transnational criminal threats. The security appeal is very strong, but this has not prevented scholars from arguing in favor of alternative solutions that would be more in line with the fundamental rights of passengers. It is clear that the data retention period is too long, and that the Directive does not guarantee the anonymity and integrity of data throughout that period. It also allows for the collection of too much material, namely sensitive data that can be used to discriminate against passengers and may have a significant impact on the lives and well-being of individuals. There is likewise some controversy regarding the identity of the third parties who can access PNR receipts. Two other issues worth highlighting in this literature review are the risks associated with modern profiling techniques, and the lack of robust notification procedures. While the Directive shows positive developments in terms of oversight and transparency in comparison to the 2011 proposal, some authors still consider it opaque and distant from passengers. A mechanism to allow them to know if, and for what reasons, their data are used is a key feature that is missing in the final version of the Directive.

These issues are echoed in the following sections and in the doctrinal claim put forward in this thesis. The next section will present the discussions of MEPs in the final steps of the legislative process, as well as the contributions of national parliaments and EU bodies to the drafting of this piece of legislation.

2. In the legislative process

Noor Huijboom and Gabriela Bodea conducted a study on PNR debates that has showed that “the power struggle between the Commission and Parliament...became less fierce”⁵⁸³ in 2005. That year, the EP started softening its stance on the PNR agenda. This might have happened

⁵⁸² Gandy, 2010: 39.

⁵⁸³ Huijboom & Bodea, 2015: 253.

because the CJEU invalidated the agreement with the US and the Commission's adequacy decision that supported it.

That struggle gave way to an institutional consensus. Huijboom and Bodea recall, however, that, while PNR appears to be a purely administrative and bureaucratic concept, it interferes with a wide range of principles, including security and privacy. Discussions in and outside the EP have dealt with a broad array of topics. Nevertheless, it appears that they have had little impact on the final text, as is apparent from the fact that the 2016 Directive is very similar to the EP's draft proposal of 2011.

Although PNR has been discussed a few times in the parliamentary term of 2014-2019, this section is limited to the debates that took place during the process for approving Directive (EU) 2016/681. This allows for a deeper look at the concerns of the advisory bodies and of the MEPs, which so far have been ignored by most scholars.

It must be recalled, nonetheless, that PNR was tabled and discussed rather hastily, following the 2016 terrorist attacks in Brussels. The debates were based on written comments by member states and advisory bodies from 2011, since the EP did not ask for new opinions. While this piece of legislation was discussed and approved in just a few days in April 2016, it had been on the table since the terrorist attacks that took place in January 2015, in Paris. There was plenty of time to review the 2011 proposal and improve it to answer both the new security demands and the fundamental rights requirements of the CFREU. As will be shown, however, the approved version does not reflect either a mature legislative process nor sufficient care for fundamental rights.

This section will first table the contributions of national parliaments. It will then put forward the main arguments present in the reports of auxiliary and supervisory entities, and will conclude with an analysis of the key topics and opinions brought to the floor by the MEPs in the hour and a half that it took them to debate PNR on 13 April 2016.

2.1 National contributions

All member states favored the approval of the Directive.⁵⁸⁴ Yet, the EP received observations from only eight national parliaments. And only three raised concerns regarding fundamental rights. They were not very sophisticated in their opinions and the main topics addressed are

⁵⁸⁴ Note from the Council of the European Union on the voting result of Directive of the European Parliament and of the Council on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (First reading) (8267/16, 25.4.2016).

also present in the literature. They talked about the tension between privacy and security, the data retention period, profiling and discrimination, and the right to notification. In any case, the EP seems to have ignored their concerns.

2.1.1 Tension and trade-off

While the tension between security and fundamental rights is extensively developed in the literature, the member states did not give it considerable importance. The Austrian National Council appealed to the Commission to pay attention to the balance between the protection of public security and respect for individual rights.⁵⁸⁵ This trade-off was also mentioned by the German Federal Council, who stressed that equilibrium between personal liberties and public security was not satisfactorily addressed in the Directive.⁵⁸⁶ However, there were no more explanations, or further arguments, backing the Austrian and German Councils' positions. They might have been on the right track, but they missed the opportunity to table a relevant claim.

2.1.2 Data retention period

The first relevant criticism concerns the length of the data retention period. The Austrian National Council argued that data should not be stored irrespective of there being concrete suspicions regarding a particular individual. Moreover, a period of five years regardless of criminal charges is in a "bestimmten Spannungsverhältnis,"⁵⁸⁷ that is, a certain tension, with the rights to privacy and data protection enshrined in the CFREU.

The German Federal Council and the Dutch Senate explored this issue in more detail. The Dutch Senate contended that holding data from innocent people might contribute to redundant profiling.⁵⁸⁸ And the German Council argued that storing data with no just cause ("Anlass"), i.e., an attributable conduct ("zurechenbar vorwerfbares Verhalten") with a dangerous nature ("Gefährlichkeit"), is a particularly serious limitation of the rights to informational self-determination and to private life. Plus, a period of five years outstrips any notion of proportionality and allows for interferences with privacy.⁵⁸⁹ As data are kept in a way that can

⁵⁸⁵ Mitteilung des Ständigen Unterausschusses des Hauptausschusses in Angelegenheiten der Europäischen Union des Nationalrates vom 5. April 2011 gemäß Art. 23f Abs. 4 B-VG, 2.

⁵⁸⁶ Beschluss des Bundesrates (6007/11), paragraph 2.

⁵⁸⁷ Mitteilung vom 5. April 2011, 2.

⁵⁸⁸ Letter from René van der Linden, president of the Senate of the States General of the Netherlands, 1.

⁵⁸⁹ Beschluss des (6007/11), paragraph 7.

be unmasked at any time, this is disproportionately long from the perspective of fundamental rights.⁵⁹⁰ The Dutch Senate made a similar remark, adding that the mechanisms to mask information present in the proposed Directive seem inappropriate, especially since the norms on the anonymization of payment data are not sufficiently tight.⁵⁹¹

2.1.3 Profiling and discrimination

For the German Council, the lack of legal certainty and publicity regarding the criteria used to assess data leaves passengers with few tools to understand processing operations and to know whether they have been negatively discriminated against. And, if different standards are applied to different people, this can render the tools intended to prevent discrimination less effective.⁵⁹²

The Dutch Senate queried the Commission about those criteria and about which data elements combined could warrant additional scrutiny.⁵⁹³ The Dutch Senate acknowledged that the PNR Directive tries to prevent the collection of sensitive data, but it remarked that other elements might indicate, for instance, a religious orientation or health situation, like meals. It also asked why nationality was not listed as a sensitive criterion, given that Article 21(2) CFREU forbids discriminatory action based on nationality.⁵⁹⁴ Regrettably, there seems to have been no reaction to these comments.

2.1.4 Right to notification

Only the German Federal Council raised concerns about the right to notification. Though an interesting point, it only observed that data subjects should be informed whenever their personal information is sent to third countries.⁵⁹⁵

2.2 Input from auxiliary and supervisory entities

The EP and the Council of the EU consulted the EESC, the EDPS, and the Committee of the Regions (COR) before initiating verbal discussions on the intra-EU PNR.

⁵⁹⁰ Beschlussdes (6007/11), paragraphs 10 and 11.

⁵⁹¹ Letter from René van der Linden, 1.

⁵⁹² Beschlussdes (6007/11), paragraph 12.

⁵⁹³ Letter from René van der Linden, 1.

⁵⁹⁴ Ibidem.

⁵⁹⁵ Beschlussdes (6007/11), paragraph 15.

2.2.1 Committee of the Regions

This Committee was the only one which did not present an opinion. On the 129th meeting of the COR's bureau, in 2011, its Commission for Citizenship, Governance, Institutional and External Affairs (CIVEX) noted that it had been requested by the Council of the EU to give an opinion to the proposal for a Directive by mid-May.⁵⁹⁶ Yet, sitting on 8 April, its secretariat gave notice that CIVEX had decided not to table opinions on two legislative proposals, PNR and the Directive on attacks against information systems.⁵⁹⁷

The COR argued that it did not provide an opinion on PNR because, from a data protection standpoint, the strategic value of this matter for municipal and regional powers seemed rather narrow. Although this may be a controversial position, the COR added that this topic could be dealt with in a wider perspective in light of the strategy for a new regulatory agenda on data protection in the Union that was foreseen for July 2011.⁵⁹⁸

PNR seemed to be secondary in the COR's political concerns. As such, anything they could say about it could be postponed for a global review of EU security. In fact, in the general comments of the policy recommendations of the COR's Opinion on the Union's internal security strategy, this Committee showed interest in measures protecting transport but pointed to previous comments censuring PNR, which, in its view, should be carefully considered by the Union legislator when delineating a EU PNR system.⁵⁹⁹ There is no other mention of PNR and there were no further developments, with the section on transport of this Opinion being mostly dedicated to land carriage.

2.2.2 European Data Protection Supervisor

The EDPS, on the contrary, was rather vocal in standing up for fundamental rights. As it had provided informal feedback throughout the development of the proposal, it gladly observed that the legislator had adopted some of its suggestions, like on data protection safeguards.⁶⁰⁰ Some

⁵⁹⁶ Agenda item 5a): Organisation of COR commission work — referrals made by the COR president, adopted by the COR at its 129th meeting, on 30 March 2011 (R/CdR 91/2011 item 5a) FR/CD/ym).

⁵⁹⁷ Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA {SEC(2010) 1122 final} {SEC(2010) 1123 final} (COM(2010) 517 final, 2010/0273 (COD), 30.9.2010).

⁵⁹⁸ Agenda item 4: Organisation of future work — decisions not to draw up opinions, adopted by the CIVEX, on 8 April 2011 (CdR 119/2011 EN/o), 3.

⁵⁹⁹ Opinion of the COR on the EU internal security strategy (CIVEX-V-018, 1.7.2011), paragraph 40.

⁶⁰⁰ Opinion of the EDPS (OJ C 181, 22.6.2011), paragraph 2.

of these consisted of making clearer the role of the PIUs, prohibiting the analysis of sensitive data, adopting the push method, and adding limits to the retention of information.⁶⁰¹

A. Harmonized system

The EDPS was not certain about the added value of a harmonized European system. Despite acknowledging that common standards improve legal security and certainty, it stressed that the Directive obliges member states to request PNR data, even if they did not do so. From this point of view, the supervisor questioned the benefit of the system to the security of personal data.⁶⁰²

What the EDPS meant was that, for data protection, the best option is not to have a PNR system at all. In fact, even if, hypothetically, data could be rendered entirely secure, it is always riskier to have data collected by law enforcement units than not having them collected at all.

B. Impact assessments

The supervisor thus called upon the legislator to present an impact assessment to review the privacy and data protection guarantees, considering how PNR impacts individual rights. It argued that an overall review was unsatisfactory.⁶⁰³ Alas, no general impact assessment was drafted for the 2016 proposal, let alone a specific one on privacy and data protection. This was not even addressed by the MEPs when discussing the proposal.

Still, it is an interesting point for reflection. This recommendation will be revisited in the concluding remarks of the thesis as it is an important lesson for the future of the EU. General impact assessments, especially if supplemented by specific impact assessments, are a crucial tool for evaluating the efficiency, efficacy, and proportionality of policies and legislation in the AFSJ. Moreover, such impact assessments should be subject to regular updates after the entry into force of the legislation to ensure that it is still necessary and proportionate, especially when it affects essential rights as PNR does.

The EDPS further remarked that including internal flights would be a broadening of the reach of the system that could jeopardize fundamental rights even further.⁶⁰⁴ Unfortunately, the supervisor gave no reasons or concrete proof to substantiate this fear.

⁶⁰¹ Opinion of the EDPS (OJ C 181, 22.6.2011), paragraph 6.

⁶⁰² *Idem*, paragraph 21.

⁶⁰³ *Idem*, paragraph 25.

⁶⁰⁴ *Idem*, paragraph 29.

C. Data retention period

The EDPS also made important comments about the data retention period. Its position on this matter was already very clear in 2011. The EDPS questioned the need and proportionality of retaining data for five years, especially seeing that these records would not be fully anonymized.⁶⁰⁵ It thus recommended that the proposal:

[S]hould be reworded [to keep] the principle of real anonymisation with no way back to identifiable data, which means that no retro-active investigation should be allowed. These data could still — and solely — be used in order to serve general intelligence purposes based on the identification of terrorism and related crime patterns in migration flows.⁶⁰⁶

It suggested that “[n]o data should be kept beyond 30 days in an identifiable form, except in cases warranting further investigation.”⁶⁰⁷ Regrettably, this was ignored in 2011 and in 2016.

D. Transparency

Finally, the EDPS said that the development of an EU PNR system aiming at the retention of all passenger data, and which works based on anonymous and volatile risk criteria, poses significant transparency issues. The worst of these is that the scheme could lead to the arrest of innocent individuals, even before the commission of criminal offenses.⁶⁰⁸

The supervisor argued that the only way to mitigate this would be to use PNR data exceptionally, only where there are real menaces based on real risk factors.⁶⁰⁹ This argument would later be echoed by the EESC⁶¹⁰ and it seems both entities believed that this could mitigate the fact that PNR depends on the massive collection of all booking elements of every passenger.

2.2.3 European Economic and Social Committee

Rodríguez García-Caro, the EESC’s rapporteur-general, stressed that it generally agreed with the opinion of the EDPS. He expressed reservations about whether fundamental rights could be

⁶⁰⁵ Opinion of the EDPS (OJ C 181, 22.6.2011), paragraphs 43 and 44.

⁶⁰⁶ Idem, paragraph 45.

⁶⁰⁷ Idem, paragraph 57.

⁶⁰⁸ Idem, paragraph 16.

⁶⁰⁹ Idem, paragraph 17.

⁶¹⁰ Opinion of the EESC (OJ C 218, 23.7.2011), paragraphs 1.3 and 3.5.

jeopardized by the proposal, as the much discussed trade-off between security and rights looked to him more like “stepping up security at the expense of citizens’ rights.”⁶¹¹ The EESC claimed that PNR came down to:

[L]egislation allowing a wide range of data about millions of citizens who have never committed any of the offences set out in the directive, and who never will, to be processed and analysed. This means that data concerning absolutely normal people will be used to establish the profiles of dangerous criminals.⁶¹²

It is unclear how the EESC knows that these individuals will never commit any offenses. Yet, what matters is that, like the EDPS, the EESC believes that PNR privileges security over privacy. While the Committee did not explore this argument, it was clear in saying that, whichever document was approved, it should guarantee the widest protection and privacy to the data processed in the system.⁶¹³

The EESC added that the Directive should have an exceptional nature. Its provisions should never contradict key principles on fundamental rights. And it further specified that this was of special importance whenever third countries sought to transfer data to other third countries.⁶¹⁴

Another interesting point was made on the technical alternatives that air carriers should use, if the common protocols for transferring data fail. This has been largely ignored by the literature. The Committee claimed that the possibility of using “any other appropriate means”⁶¹⁵ is not entirely suitable. In its view, the legislator should have provided concrete information on exactly which alternative means are adequate for transferring data.⁶¹⁶ Regrettably, this flaw is still present in the 2016 version of the Directive, which leaves the door open to security risks.

Just like the EDPS, the EESC did not discuss many other problems arising from the PNR Directive. Yet, it concluded with a note on transparency. It suggested that it should contain a mandatory traceability mechanism so that access and processing would be registered.⁶¹⁷ The purpose would be to make it possible to determine who accesses PNR data at any time.⁶¹⁸ It must be noted that this safeguard has been added in 2016. The PIUs are now obliged to keep records of all operations performed upon the data.⁶¹⁹

⁶¹¹ Opinion of the EESC (OJ C 218, 23.7.2011), paragraphs 1.1 and 1.2.

⁶¹² *Idem*, paragraph 3.3.

⁶¹³ *Idem*, paragraph 3.7.

⁶¹⁴ *Idem*, paragraph 4.8.

⁶¹⁵ Article 16(1) of Directive (EU) 2016/681.

⁶¹⁶ Opinion of the EESC (OJ C 218, 23.7.2011), paragraph 4.5.

⁶¹⁷ *Idem*, paragraph 3.9.

⁶¹⁸ *Ibidem*. See also paragraph 4.10.

⁶¹⁹ Articles 13(5) and (6) of Directive (EU) 2016/681.

2.3 The debate in the European Parliament

Sitting on 13 April 2016, the EP debated the PNR proposal before approving it at first reading on the following day. 43 MEPs intervened. There were also questions tabled under the blue card prerogative and seven written declarations. Yet, not all speakers were clear on where they stood on the issues arising, and few engaged with fundamental rights in a shrewd way.

2.3.1 The kick-off

The opening and end of the debate were led by Timothy Kirkhope, the rapporteur of the LIBE Committee for PNR. He considered that only through a common legal instrument at EU level would it be possible to protect individual privacy. He opened the debate arguing in favor of its approval, although he did not explain how the Directive protects passengers. His concern was that broad protection would not be ensured if member states were left to regulate PNR.⁶²⁰

Kirkhope's position was backed by Dimitris Avramopoulos, the MEP representing the Commission in the discussions. He was confident that the Directive had been drafted to arrive at the best equilibrium between privacy and security, through a set of robust safeguards. He referred to the limited conditions on data access and transfer, the controlled retention period with anonymization mechanisms, the prohibition on storing sensitive data, and the obligation to delete them, as well as to the supervision of the DPOs and national independent entities.⁶²¹

2.3.2 Tension and trade-off

The balance between security and privacy was mentioned throughout the whole debate. Most MEPs speaking in favor of the Directive addressed this trade-off. Still, they often referred to data protection guarantees built into its text without concretely looking at its draft norms, or discussing how they safeguard fundamental rights. Almost all, in fact, considered the balance between privacy and security adequate in the proposal, without going into much detail. Only a few clarified their views by reference to specific examples, which reveals a gap between the arguments of the MEPs and the functioning of PNR.

⁶²⁰ Intervention by Timothy Kirkhope on the debate on the Use of Passenger Name Record data (EU PNR), sitting of the European Parliament of 13 April 2016.

⁶²¹ Intervention by Dimitris Avramopoulos on the debate on the Use of Passenger Name Record data (EU PNR), sitting of the European Parliament of 13 April 2016.

A. For security

Michał Boni, of the European Conservatives and Reformists Group (ECR), was, perhaps, the most sophisticated intervener pro security, considering that:

[T]he masking-out of data after six months...[establishing] monitoring mechanisms...and a list of serious crimes [as well as having a section on] the role of national data protection authorities [and] the obligation of appointing a data protection officer [are examples of the] many data protection safeguards and principles that guarantee respect for fundamental rights.⁶²²

He tried to demonstrate how the proposal directly tackled security without waiving individual privacy. However, Boni might have gone too far in claiming, based on no examples, that data, privacy, freedom, and security are all equally protected and given the same relevance in the Directive.

There was a sort of haste in the interventions of some MEPs who tried to lessen the relevance of privacy concerns, while persuading the EP to approve the proposal. These interventions recurrently used the Brussels terrorist attacks to argue that the debate should not be delayed any further. Helga Stevens, also of the ECR, for instance, finished her intervention with a call to common sense, saying that she saw no reason to delay, or even to vote against, PNR.⁶²³ This is an important aspect to highlight from the debate. To use those dreadful events was a persuasive strategy, and it may have pressured many MEPs into believing that they needed to approve PNR, regardless of its flaws, in order to ensure the safety of EU citizens. To vote against would, therefore, be seen almost as a criminal act in itself. Yet, this rhetoric needs careful study. Hastening parliamentarians into approving security legislation in the aftermath of criminal events with a large impact on social media and public opinion will be revisited in the conclusion of the thesis. It indicates a relevant lesson underlying the journey of the PNR Directive.

Along this line of thought, Christel Schaldemose, of the Group of the Progressive Alliance of Socialists and Democrats (S&D), admitted that PNR's deficiencies were corrected by the data protection package. She agreed that there should be a more controlled retention of data but, shortly after, Schaldemose added that MEPs had to be pragmatic in terms of finding a

⁶²² Intervention by Michał Boni on the debate on the Use of Passenger Name Record data (EU PNR), sitting of the European Parliament of 13 April 2016.

⁶²³ Intervention by Helga Stevens on the debate on the Use of Passenger Name Record data (EU PNR), sitting of the European Parliament of 13 April 2016.

balance between the protection of private life and the protection of citizens against terrorism and organized crime.⁶²⁴

The call for such balance was echoed by other members of the S&D, such as Christine Bonnefoy and Juan López Aguilar. Bonnefoy stated that PNR should be “efficace et opérationnel, juste et proportionné, [but also a measure] qui assure la protection des libertés individuelles, en particulier le respect de la vie privée.”⁶²⁵ And like her colleague, Schaldemose, she saw its implementation at the same time as the data protection package as a strong guarantee of this balance. This was reiterated by López Aguilar, who stressed that the EP was being unfairly accused of dragging its feet regarding PNR. In his view, “privacidad es un derecho fundamental de los europeos, garantizado como tal en la Carta de los Derechos Fundamentales [and the approval of the GDPR] puede ser útil en la garantía de un equilibrio razonable entre libertad y seguridad para los ciudadanos europeos a los que representamos.”⁶²⁶ Curiously, it could be said that, from this angle, these MEPs did not believe that the PNR Directive included sufficient guarantees to ensure privacy and individual liberties, but that this was somehow made tolerable by the simultaneous approval of the GDPR.

Esteban González Pons, of the European People’s Party (EPP), likewise used the trade-off idea, but ended up making a controversial argument. He distanced himself from those who believed the right to privacy of terrorists was more important than the right to life of potential victims. He emphasized that citizens already relinquish their privacy in order to pay taxes, with fiscal authorities having access to troves of relevant data. Analogously, he said he would be willing to abdicate part of his privacy to save his own life. In a rather populist move, González Pons balanced the rights to life and to private life and concluded that the main priority of MEPs should be the former.⁶²⁷

B. For privacy and data protection

Most of those who presented ideas against the approval of the Directive were not very sophisticated in replying to the previous remarks, or in deconstructing the problems that could

⁶²⁴ Intervention by Christel Schaldemose on the debate on the Use of Passenger Name Record data (EU PNR), sitting of the European Parliament of 13 April 2016.

⁶²⁵ Intervention by Christine Bonnefoy on the debate on the Use of Passenger Name Record data (EU PNR), sitting of the European Parliament of 13 April 2016.

⁶²⁶ Intervention by Juan López Aguilar on the debate on the Use of Passenger Name Record data (EU PNR), sitting of the European Parliament of 13 April 2016.

⁶²⁷ Intervention by Esteban González Pons on the debate on the Use of Passenger Name Record data (EU PNR), sitting of the European Parliament of 13 April 2016.

ensue from PNR systems. Still, some MEPs raised issues that are worth recalling. Sophia In't Veld, for example, of the Alliance of Liberals and Democrats for Europe (ALDE), argued that it gave a false sense of security⁶²⁸ which undermined the whole discussion on fundamental rights. She was backed by Jan Phillip Albrecht, of the Greens and European Free Alliance (EFA), who stated that the EP was tabling nothing more than a symbolic policy which would take a heavy toll on the security and rights of citizens.⁶²⁹

The risk of jeopardizing citizens' freedoms was also emphasized by other MEPs,⁶³⁰ with Albrecht adding that PNR violates privacy because of its blanket data retention, i.e., the capacity of the system to broadly and indiscriminately collect huge amounts of information. Although not pinpointing concrete case law, he ended his intervention by highlighting that both the CJEU and the ECtHR have consistently observed that putting everyone under control violates individual rights and freedoms.⁶³¹

While initially appearing to be in favor of PNR, Beatrix Von Storch, of the Europe of Freedom and Direct Democracy (EFDD), remarked that it is "eine gigantische Vorratsdatenspeicherung,"⁶³² a gigantic data retention system that violates privacy. In her visual description, it is about the data of those who flew where and when, who sat next to whom, who ate what, how they paid for the trip, and so on. It consists of data stored about everyone for no proper reason, and then made accessible to law enforcement authorities.

Notis Marias, from the ECR, also positioned himself emphatically as against PNR. He said that security should serve freedom and not make it a hollow concept. In an interesting point, Marias added that the trade-off between freedom and security was unbalanced in the proposal since security was not serving freedom, or respecting the core of individual rights. It not only disrespected personal data guarantees but actually circumvented them. He concluded by criticizing the EP if, under the pretext of terrorism, it managed to approve a policy which, he believed, should be used only in emergency scenarios and under strict conditions.⁶³³

⁶²⁸ Intervention by Sophia In't Veld on the debate on the Use of Passenger Name Record data (EU PNR), sitting of the European Parliament of 13 April 2016.

⁶²⁹ Intervention by Jan Phillip Albrecht on the debate on the Use of Passenger Name Record data (EU PNR), sitting of the European Parliament of 13 April 2016.

⁶³⁰ For instance, in the intervention by Marie-Christine Vergiat on the debate on the Use of Passenger Name Record data (EU PNR), sitting of the European Parliament of 13 April 2016.

⁶³¹ Intervention by Jan Phillip Albrecht on the debate on the Use of Passenger Name Record data (EU PNR), sitting of the European Parliament of 13 April 2016.

⁶³² Intervention by Beatrix Von Storch on the debate on the Use of Passenger Name Record data (EU PNR), sitting of the European Parliament of 13 April 2016.

⁶³³ Intervention by Notis Marias on the debate on the Use of Passenger Name Record data (EU PNR), sitting of the European Parliament of 13 April 2016.

Marju Lauristin, of the S&D, used her blue card prerogative to ask Monika Hohlmeier, of the EPP, why there were so many limitations to the functions and tasks of the DPOs. It is, however, not clear whether Lauristin was comparing the final version with previous drafts, or with the external agreements. In any case, the answer was that the control mechanisms and data protection standards were set very high in terms of how the algorithms could be used to search for the most serious criminals. It was a rather vague answer, but Hohlmeier further commented that data protection guarantees would be reviewed in five years, if necessary.

2.3.3 Data rights and transparency

There were no significant references to profiling, or discrimination, in the debate. And only a few MEPs addressed data rights and transparency. In his opening words, Kirkhope claimed that the Directive contemplates specific rights of redress that he feared would not be considered if PNR was left to the member states to regulate.⁶³⁴ Yet, he failed to explain why he thought member states would omit rights of redress in their national proposals. Despite this, Anna Bildt, of the EPP, backed his idea and added that a EU PNR system is a guarantee of more transparency. In her view, a single scheme makes the circulation of data known to passengers and ensures harmonized protection in all member states.⁶³⁵

On the opposing side, Marju Lauristin put a second question to Monika Hohlmeier. This time, she asked why the EPP opposed the idea of letting air passengers know about their rights and how data are collected and processed.⁶³⁶ Hohlmeier replied this was false, and Lauristin missed the opportunity to further elaborate on PNR's transparency issues.

2.3.4 Wrapping-up

Most speakers were in favor of PNR, and the majority of MEPs who participated were from the EPP. In total, 15 members of this group voiced their concerns, and all said they would vote in favor of the proposal. Four others provided written declarations, but were likewise pro approval. Three EP groups were divided. Six members of the S&D voiced their support for PNR, while

⁶³⁴ Intervention by Timothy Kirkhope on the debate on the Use of Passenger Name Record data (EU PNR), sitting of the European Parliament of 13 April 2016.

⁶³⁵ Intervention by Anna Bildt on the debate on the Use of Passenger Name Record data (EU PNR), sitting of the European Parliament of 13 April 2016.

⁶³⁶ Intervention by Marju Lauristin on the debate on the Use of Passenger Name Record data (EU PNR), sitting of the European Parliament of 13 April 2016.

one said he would vote against. Two others provided written declarations in which they showed that they were in favor of the proposal. The same happened with ALDE, with five MEPs for and one against, and the ECR, with three in favor and one against. The remaining parties expressed their opposition to PNR, but they were not as vocal as the members of the supporting parties. Three MEPs spoke from the Confederal Group of the European United Left/Nordic Green Left, with two others from the Greens/EFA, one from the Europe of Nations and Freedom, and one from the EFDD, with another from this party providing a written declaration arguing against PNR.

The bulk of the arguments was not very refined from either side, and the fundamental rights of air passengers affected by PNR were often far from the core of the debate. There was little time to intervene in these discussions, but it is unfortunate that most MEPs did not manage to direct the spotlight onto the key issues concerning rights and freedoms.

This first part of chapter 3 has provided us with a very broad set of findings. More arguments have been made by scholars, MEPs, and other actors. Those tabled here are just the most relevant for the purposes of this research. The next part will sift through the judgements and opinions of the CJEU in much the same way, so that the legal analysis provided at the end of the chapter examines the most solid arguments and the most promising observations, in order to challenge the validity of the PNR Directive.

The overall argument of the thesis benefits greatly from the literature review and this survey into the legislative process relating to the intra-EU PNR. The debate in the EP was brief and poor. The engagement with the draft text of the Directive was relatively thin and, on account of this, there were relevant shortcomings in how the MEPs addressed the fundamental rights dimension of PNR. This engagement is an aspect that will merit close attention in the doctrinal claim put forward in chapter 3.3. Despite strong warnings from supervisory bodies, the EDPS above all, most MEPs ignored key problems which had been discussed since 2011, like the risks of collecting sensitive data, and the lack of individual notification. Still, the length of the data retention period is, probably, the best example of a problem that was anticipated, but did not resonate in the legislative debate. The MEPs maintained the heavily criticized period of five years, in the belief that the data protection safeguards, the depersonalization mechanisms, and the powers of DPOs would suffice to guarantee the integrity and security of data. It is also notable that the approval of the GDPR at the same time led many parliamentarians to believe that this piece of legislation would be able to counteract certain flaws of the Directive.

There are, in any case, also positive aspects worth stressing. Concerns raised regarding access conditions, data transfers, or supervision by national independent bodies have been

included as legal norms. It is not clear whether the MEPs were influenced by the views of national parliaments or auxiliary bodies, since there was no mention of their contributions in the debate. Still, some provisions reveal a connection with such contributions. The EESC had suggested that the system should include a traceability mechanism to identify and trace access, for example, and PIUs are now obliged to keep a record of data processing operations.

Many, if not all, of the arguments put forward by the MEPs have been discussed in the literature. They too refer to the balance and trade-off between security and fundamental rights, the advantages of having a unified PNR system at EU level, the need to inform passengers of how their data are handled, and the risks of having law enforcement agents collect large troves of personal information. To have different actors mention certain topics and express common fears is a good indicator that there are material to be researched and arguments to be explored. They will be the building blocks for the legal analysis that is now taking form.

Chapter 3.2

Trumping fundamental rights: Stopover

“The European Court of Justice has long required the Community to respect fundamental rights...Thus, in diverse ways, the European Union has acknowledged that it has an important role to play in promoting respect for the human rights of its citizens and of all others resident within the Union and of ensuring that those rights are fully respected...[Yet,] the European Court of Justice, no matter how carefully it may be attuned to the need to ensure full respect of fundamental rights within the Community legal order, cannot make up for the absence of the necessary legal and policy commitments on the part of the other institutions.”⁶³⁷

Introduction

This is the second part of the thematic chapter on fundamental rights. It looks at case law of the CJEU.⁶³⁸ Its structure and findings will then be used to assess the Directive, and the question of whether it has disregarded key rights enshrined in EU primary law. This part examines the judgment declaring the invalidity of Directive 2006/24/EC (commonly known as ‘Digital Rights Ireland’⁶³⁹) and the Opinion on the 2014 EU-Canada PNR Agreement (‘Opinion 1/15’).

Opinion 1/15 is frequently cited in discussions about fundamental rights and PNR.⁶⁴⁰ It is seen by some as a key example of how the CFREU is asserting its place in the Union’s external policies.⁶⁴¹ Still, it has also attracted criticism for resembling a rewording of the PNR Agreement.⁶⁴² That debate is beyond the scope of the present work.⁶⁴³ It is, however, important

⁶³⁷ Alston & Weiler, 1998: 666 and 668.

⁶³⁸ It emulates the scheme of analysis used by the CJEU which, according to Andrew Roberts, follows the method applied in the jurisprudence of the ECtHR. In case *S. and Marper v the United Kingdom*, 4 December 2008 (30562/04 and 30566/04), the ECtHR asked “the following questions: (i) what is the nature of the right at issue? (ii) what is the nature of the interference with the right? (iii) how serious is the interference? (iv) what is the object pursued by the interference? These questions, if tackled sequentially, provide a logical and coherent framework for thinking about the function and limits of a right to privacy” (Roberts, 2015: 540).

⁶³⁹ Joined cases C-293/12 and C-594/12.

⁶⁴⁰ Kuner, 2017.

⁶⁴¹ Tambou, 2018: 189. See also Tracol, 2014: 745, Peyrou, 2017, or Tinière, 2018. Ojanen, 2014: 529, has, curiously, stressed the role of the CFREU in joined cases C-293/12 and C-594/12. He finds them to be crucial for fundamental rights and EU constitutional theory, stating that this jurisprudence “indicates both the ability and willingness of the Court to embark on a very rigorous rights-based review of EU legislative measures in light of the EU Charter of Fundamental Rights. Moreover, the judgment features as a continuation of such constitutional dynamics that have significantly strengthened the status of fundamental rights within the EU legal order in recent years, as well as transformed the overall appearance of the Court from an economic court towards a supranational constitutional court that has actually become a judicial forerunner for the protection of fundamental rights in the area of counter-terrorism.”

⁶⁴² Lord, 2019: 265. Zalnieriute, 2018: 1047, has even called it “a ground-breaking example of law-making, with important implications for many areas of EU law, the future of the EU legal framework for the PNR agreement, as well as international data transfers and transatlantic data relations more generally.”

⁶⁴³ Vedaschi, 2018: 427, for instance, claims that “[t]he Court of Justice...did something...that is worth remarking upon: in carefully analysing the text of the Agreement, even censuring its wording, it engaged in a task that could be defined as ‘borderline’ to that of a legislative drafting committee. The Court suggested the correct way to redraft

at this moment to highlight how Directive 2006/24/EC has, oddly, been left out of most commentaries on the intra-EU PNR system.

Directive 2006/24/EC, challenged in *Digital Rights Ireland*, is also known as data retention Directive and it tabled a system that would be copied by the PNR Directive in terms of blanket collection, retention, and processing of personal data on a massive scale for investigative purposes.⁶⁴⁴ As Luisa Marin wrote, PNR is close to the data retention Directive since they both allow for the unprecedented collection of personal data from innocent individuals.⁶⁴⁵

Its invalidation is seen as a landmark in the case law on fundamental rights.⁶⁴⁶ The Council of the EU said it was a critical ruling for the future of EU action on privacy and data protection matters.⁶⁴⁷ This is mostly due to the fact that the Court outlawed general surveillance practices of EU citizens and laid out concrete criteria for the Union and the member states to enact legislation compliant with EU primary law.⁶⁴⁸ It is a decisive ruling, in Federico Fabbrini's view, on the expansion of the Court's supervision over governmental surveillance⁶⁴⁹ — a type of surveillance which would later resurface with the European PNR.

Some authors have raised concerns about the compatibility of the PNR Directive with the

the Agreement to other EU institutions, not only by way of principled declarations, but also by proffering concrete examples of the words and phrases to be substituted. This high rate of 'intrusiveness' can be related to the gist of this decision, which can be synthesised as follows. Conceiving a legal framework in which surveillance has no role would be utopian, given the seriousness of the current terrorist threat; nonetheless, mass surveillance must be kept subject to particularly strict rules. Against this background, if the policy-maker proves unable to remain within these limits and to guarantee that individual rights will not be totally sacrificed in the name of security, courts will be increasingly called to play a pivotal role, even going beyond their institutional attributions and bearing quasi-legislative (and political) responsibility." On a similar note, Hijmans, 2017: 410, remarks that "the opinion positions the CJEU as a sort of co-legislator. The precise scrutiny by the Court — almost article-by-article — raises the question [on] whether the Court does not acquire features of the legislator." See also Pfersmann, 2002: 789 ff. Differently, Mendez, 2017: 812, contends that "rather than criticise the Court for its detailed scrutiny of the Canada PNR Agreement, we should praise it for seeking to ensure that the privacy and data protection standards in the Charter are taken seriously and that, despite the very real threat of terrorism and serious crime, international agreements cannot simply be used in a manner that rides roughshod over these fundamental rights."

⁶⁴⁴ See Maras, 2012, for a reflection on the Directive as part of the general trade-off between security, civil liberties, and fundamental rights. The author also looks at some of its relevant social consequences.

⁶⁴⁵ Marin, 2016: 225.

⁶⁴⁶ This has been stressed by considerable literature over the years, namely Granger & Irion, 2014: 841, Ojanen, 2014: 529, Spina, 2014: 250, Stoeva, 2014: 590, Benedizione & Paris, 2015: 1757, Fabbrini, 2015: 72, Lynskey, 2015: 166, Mitsilegas, 2015: 39, Roberts, 2015: 536, Vainio & Miettinen, 2015: 300, Marin, 2016: 211, or Silveira & Freitas, 2017: 62. On an interesting note, Bignami, 2007, for instance, considered that the data retention Directive was sufficient to safeguard privacy rights.

⁶⁴⁷ Information Note from the General Secretariat of the Council to the Permanent Representatives of the Committee and Council on the judgment of the Court of 8 April 2014 in joined cases C-293/12 and C-594/12 – *Invalidation of 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 (9009/14, 5.5.2014)*, paragraph 19.

⁶⁴⁸ Marin, 2016: 223. This is, nonetheless, a contested matter, as demonstrated by Vainio & Miettinen, 2015: 299 ff. From their analysis, some member states and authors believe that blanket data retention can, in certain cases, be acceptable and lawful to fight crime and terrorism, while being in line with the CFREU.

⁶⁴⁹ Fabbrini, 2015: 73.

judgment in *Digital Rights Ireland*.⁶⁵⁰ But these concerns are not sufficiently consolidated in the literature and institutional discussions. The invalidation of the data retention Directive was based on issues that are present in PNR because EU legislative bodies overlooked key problems mentioned in the case law. This is a key finding that will be revisited as a broader lesson in the conclusion to this thesis. If, as AG Mengozzi contends, Opinion 1/15 has consequences for the future of the EU PNR system,⁶⁵¹ this is no less true for the ruling of the Court in joined cases C-293/12 and C-594/12.⁶⁵²

There are other judgements regularly mentioned when discussing privacy and data protection, but no case law is as pertinent as that which is considered here. As exemplified by Arianna Vedaschi,⁶⁵³ in joined cases C-203/15 and C-698/15,⁶⁵⁴ for instance, the CJEU addressed a preliminary ruling on a data retention scheme foreseen by national legislation. And, in case C-362/14,⁶⁵⁵ it declared an adequacy decision issued by the Commission invalid. Neither case was about PNR, or about legislation regulating data-based systems at EU level. They, and many others, will be used to help explore the views of the Court, but joined cases C-293/12 and C-594/12 and Opinion 1/15 seem the most important rulings to study in depth to assess the validity of Directive (EU) 2016/681. Plus, they are rather important decisions for understanding data protection in a broader, deeper sense.⁶⁵⁶

This part is structured in accordance with the case law. It is divided into two major sections, each corresponding to those Court rulings. They are assessed chronologically and, just as the judges did, the analysis takes a small-step approach in identifying the interferences with the rights to privacy and data protection of those EU legal acts. The sections question whether there is a serious interference and whether it is provided for by law, encroaches upon the essence of those rights, and serves objectives of general interest recognized by the Union. The last subsections apply proportionality tests to such interference, assessing its compliance with the criteria of adequacy and strict necessity.

These are the crucial elements reviewed by the judges in the case law and they are analyzed here, even if the Court rulings are not entirely summarized. Though the findings result from a comprehensive appraisal of the jurisprudence, there would be no space or need to review the

⁶⁵⁰ Marin, 2016: 225.

⁶⁵¹ Opinion of AG Mengozzi, paragraph 4.

⁶⁵² The first time that the CJEU “invalidated EU secondary legislation in its entirety on the basis of the Charter” (Kuner, 2018: 857 and 858). See also Fennelly, 2019: 683, and Marin, 2016: 211.

⁶⁵³ Vedaschi, 2018: 411. See also Zalnieriute, 2018: 1053 ff.

⁶⁵⁴ Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, 21 December 2016 (ECLI:EU:C:2016:970).

⁶⁵⁵ C-362/14, *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015 (ECLI:EU:C:2015:650).

⁶⁵⁶ Kuner, 2017.

cases in full. In fact, just like the previous chapter, the proportionality assessments only focus on key issues that can then be used to further evaluate the intra-EU PNR system. These issues are the quantity and quality of collected data, the data retention period, access rights by third parties, and individual data rights, especially the right of air passengers to notification.

This is a methodological approach suited to this project, as it uses complementary sources to help build specific and robust claims, rather than broad remarks which only vaguely critique the Directive. The doctrinal viewpoint taken in this chapter rests on a multilayered approach combining case law, literature, and policy discussions, differentiating it from previous works on the matter.

1. Joined cases C-293/12 and C-594/12

In case C-293/12, the referring Court, the High Court of Ireland, asked the CJEU directly about the privacy and data protection rights of citizens.⁶⁵⁷ It queried whether Directive 2006/24/EC was compatible with the right to privacy enshrined in Articles 7 CFREU and 8 of the European Convention of Human Rights.⁶⁵⁸ It also asked about its compatibility with the right to data protection, foreseen in Article 8 CFREU.⁶⁵⁹

This case was joined with case C-594/12 because the Constitutional Court of Austria had similar concerns about the compatibility of the Directive with the CFREU since it provided for the long-term storage of data from countless individuals. For the *Verfassungsgerichtshof*, those most likely to be affected by this system of phone data retention were consumers whose behavior did not warrant the collection of their personal data. It exposed them:

To a greater risk that authorities [would] investigate the data relating to them, become acquainted with the content of those data, find out about their private lives and use those data for multiple purposes, having regard in particular to the unquantifiable number of persons having access to the data for a minimum period of six months.⁶⁶⁰

⁶⁵⁷ Joined cases C-293/12 and C-594/12, paragraph 18.

⁶⁵⁸ Article 7 CFREU copies Article 8(1) ECHR. Its number 2, however, adds criteria to assess potential interferences with this right, stating that “[t]here shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

⁶⁵⁹ Joined cases C-293/12 and C-594/12, paragraph 18. The following questions tabled before the CJEU concerned freedom of expression (Article 11 CFREU) and the right to good administration (Article 41 CFREU). They are not going to be assessed here since the Court declined to examine the validity of Directive 2006/24/EC on the basis of Article 11 (paragraph 70) and was silent regarding Article 41.

⁶⁶⁰ Joined cases C-293/12 and C-594/12, paragraph 20.

Above all, it found this to be a matter of proportionality. It thus asked for a preliminary ruling to determine whether “Articles 3 to 9 of [Directive 2006/24/EC were] compatible with Articles 7, 8 and 11 [CFREU].”⁶⁶¹ AG Cruz Villalón would claim that he firmly believed that the data retention Directive by itself violated privacy.⁶⁶²

The CJEU joined the questions referred by these courts and discussed data protection together with privacy.⁶⁶³ It claimed that private telecommunications providers storing the personal information of customers interfered with both rights, not least because providers processed data and Article 8(1) CFREU regulates data processing activities.⁶⁶⁴

Some scholars have criticized this view. They doubt the added value of discussing data protection since the case law does not treat it as autonomous from privacy. Others expected a more sophisticated justification. Xavier Tracol finds it unimpressive and even naïve,⁶⁶⁵ while Orla Lynskey remarks that:

[G]iven the overlap between the two rights, it can be seen that there is little to be obtained by incorporating data protection analysis in the Court’s judgment. It is suggested that the outcome of the proceedings would have been identical had the case been decided on the basis of the right to privacy alone.⁶⁶⁶

This observation reveals a fundamental criticism. It is often unclear in the case law how EU secondary law interferes with the right to data protection separately from the right to privacy. Data protection usually comes as an appendix to privacy. If privacy is affected, data protection is affected as well, without a robust theoretical justification. The Court often disregards the legal autonomy of the concept of data protection and its specific scope in primary law.

Maria Tzanou finds that this assertion suggests that any data processing operation causes the application of Article 8 CFREU and immediately leads to its violation, even when such operations comply with the standards set out in its numbers 2 and 3. Still, this is an impractical approach as everything relates to data protection,⁶⁶⁷ making it very difficult to assess the quality of data protection safeguards in secondary law through the lens of the jurisprudence.

Curiously, she adds that the Court addressed each fundamental right individually, which might indicate that it sees data protection as a separate and independent right, not a subsection

⁶⁶¹ Joined cases C-293/12 and C-594/12, paragraph 21.

⁶⁶² Opinion of AG Cruz Villalón, delivered on 12 December 2013 (ECLI:EU:C:2013:845), paragraph 68.

⁶⁶³ Joined cases C-293/12 and C-594/12, paragraphs 29 and 30.

⁶⁶⁴ *Idem*, paragraph 36.

⁶⁶⁵ Tracol, 2014: 743. He further added that this “shortcoming of the judgment does not imply that the finding of the Grand Chamber is legally erroneous but simply shows the weakness of its reasoning on this specific point.”

⁶⁶⁶ Lynskey, 2015: 169.

⁶⁶⁷ Tzanou, 2017: 63.

of the right to privacy.⁶⁶⁸ Yet, it did not use separate arguments to justify how the scope of data protection was interfered with. As such, Tzanou concludes that, in substantive terms, the CJEU's assessment of what is an interference with data protection seems to be rather superficial.⁶⁶⁹ It seems the Court followed Elitsa Stoeva in believing that data protection is indivisible from privacy.⁶⁷⁰ Hitherto, this is not true. There is an evident connection between these rights but they have distinct scopes and purposes.

As mentioned before, the first step taken by the judges was to assess the type of interference with fundamental rights. The idea was to determine which provisions in the data retention Directive provoked a serious interference with privacy and data protection.

1.1 Serious interference

The Court began by stating that data collected could allow persons with access rights to:

[K]now the identity of the person with whom a subscriber or registered user ha[d] communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place, [together with the] frequency of the communications...with certain persons during a given period.⁶⁷¹

As such, those with access rights could depict a rather detailed impression of the lives of data subjects, namely concerning their behaviors, whereabouts, daily routines, and even social and personal connections.⁶⁷²

1.1.1 Was there an interference?

Retaining personal data to allow law enforcement authorities access openly affects private lives in a particular way.⁶⁷³ This was the Court's position, namely that this interference shattered the

⁶⁶⁸ Tzanou, 2017: 59. Elitsa Stoeva, 2014: 578, recalls that the Court has recognized the right to have personal data protected as a fundamental right even before the CFREU was given the normative value of primary law. This makes the slow development of the jurisprudence even more puzzling. She was thinking of case C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU*, 29 January 2008 (ECLI:EU:C:2008:54).

⁶⁶⁹ Idem: 59.

⁶⁷⁰ Stoeva, 2014: 577.

⁶⁷¹ Joined cases C-293/12 and C-594/12, paragraph 26.

⁶⁷² Idem, paragraph 27. See, by analogy, joined cases C-203/15 and C-698/15, paragraph 99, and C-511/18, C-512/18 and C-520/18, paragraph 117.

⁶⁷³ Idem, paragraph 29.

privacy-centered view of Directives 95/46/EC and 2002/58/EC. Unlike the data retention Directive, they:

Provide[d] for the confidentiality of communications and of traffic data as well as the obligation to erase or make those data anonymous where they [were] no longer needed for the purpose of the transmission of a communication, unless they [were] necessary for billing purposes and only for as long as so necessary.⁶⁷⁴

This idea was first put forward by AG Cruz Villalón.⁶⁷⁵ It seems the Court thought the data retention Directive could create a new paradigm on privacy, a paradigm that endangered the classic European approach to protecting individual rights.

The Court further declared that ascertaining that the right to privacy has been violated⁶⁷⁶ is independent from the sensitivity of certain data, and even from individuals being aware of the interference.⁶⁷⁷ This line of reasoning has been consolidating in the case law,⁶⁷⁸ following the jurisprudence of the ECtHR.⁶⁷⁹ The judges therefore concluded that having providers of online and telecommunications services collect personal data of an intimate nature from consumers constituted, per se, an interference with Article 7 CFREU.⁶⁸⁰ There was no need to assess whether those data were sensitive, or to find out if telecommunications users would sustain concrete disadvantages as a result of having their data processed.

Martin Nettesheim interestingly remarked that the Directive only created “a *threat potential*.”⁶⁸¹ This means that the CJEU found an interference with privacy, even though it was almost certain that none of the personal data of most individuals would be used.⁶⁸² Nettesheim

⁶⁷⁴ Joined cases C-293/12 and C-594/12, paragraph 32.

⁶⁷⁵ Opinion of AG Cruz Villalón, paragraph 39.

⁶⁷⁶ Joined cases C-293/12 and C-594/12, paragraph 33.

⁶⁷⁷ Data can be sensitive also depending on the context and use they are given. Yet, certain data, especially very personal information that is not anonymized or aggregated, tend to be considered objectively sensitive, such as financial or health data. See also cases C-623/17, paragraph 70, and C-511/18, C-512/18 and C-520/18, paragraphs 115 and 116.

⁶⁷⁸ Joined cases C-465/00, C-138/01 and C-139/01, *Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauerermann (C-139/01) v Österreichischer Rundfunk*, 20 May 2003 (ECLI:EU:C:2003:294), paragraphs 74 and 75.

⁶⁷⁹ Case *Amann v Switzerland*, 16 February 2000 (27798/95). In that case, the Swiss Federal “Public Prosecutor’s Office [had drawn] up a card on the applicant for its national security card index” (paragraph 10) after a business call he had received had been intercepted due to police suspicions of communist connections (paragraph 22). The ECtHR argued that it was “not for the Court to speculate as to whether the information gathered on the applicant was sensitive or not or as to whether the applicant had been inconvenienced in any way. It [was] sufficient for it to find that data relating to the private life of an individual were stored by a public authority to conclude that, in the instant case, the creation and storing of the impugned card amounted to an interference, within the meaning of Article 8 [ECHR], with the applicant’s right to respect for his private life” (paragraph 70).

⁶⁸⁰ Joined cases C-293/12 and C-594/12, paragraph 34.

⁶⁸¹ Nettesheim, 2015: 61.

⁶⁸² This broad understanding of the concept of interference would be later criticized by Georgios Dimitropoulos when commenting on Nettesheim’s paper. In his view, it caused many legal and concrete problems. These authors

and the Court presented no statistical data to support their claims. Yet, they are based on how law enforcement operations are undertaken, and the fact that only a limited number of people is usually investigated for criminal purposes. It seems the judges were careful here. They agreed that even a small possibility of data being used might endanger the rights and freedoms foreseen in the CFREU.⁶⁸³ As such, the CJEU had to find that the data retention Directive had the power to interfere with personal liberties.⁶⁸⁴

The Court considered that its claims also applied regarding the right to data protection.⁶⁸⁵ In fact, the Directive regulated the responsibilities of service providers on how they retained the data they produced or processed.⁶⁸⁶ It encompassed activities involving the processing of data.

base their opinions on the theoretical distinction they distil from the case law of the CJEU between retention of, and access to, data. In Dimitropoulos words, “[i]f the distinction between ‘retention’ by the communications providers and ‘access’ by the authorities is followed systematically, it could be argued that the retention alone does not constitute an interference with fundamental rights. The initial retention occurs, one way or another, for logistics reasons of the communications companies that keep our data for billing and customer service purposes...If one agrees to such a definition of intervention, then one has to be stricter with the assessment of the provision of access to the data by the national authorities” (Dimitropoulos, 2015: 77). This argument is not free from controversy, but a distinction between access and retention should be kept in mind. There are different degrees of interference and encroachment with fundamental rights in distinct phases of processing. However, retention implies access and, on the other hand, Dimitropoulos forgets the impact on the right to data protection of having data incorrectly stored and accessible for later use. Retaining data without sufficient safeguards can be highly dangerous for their integrity and for the privacy of data subjects. In any case, this seems more a matter of degree of data security rather than a matter of privacy, contrary to what these authors suggest. Having third parties accessing personal data tends to interfere with privacy regardless of whether they are private or public bodies. It is the different purposes for which data can be used and the implemented safeguards that are the key issues.

⁶⁸³ This idea has been consolidating in the case law, leading the CJEU to acknowledge that even the simple retention of information may lead to interferences, and potentially unlawful interferences, with fundamental rights. For instance, in joined cases C-511/18, C-512/18 and C-520/18, paragraph 119, the judges wrote that “[i]n view of the significant quantity of traffic and location data that may be continuously retained under a general and indiscriminate retention measure, as well as the sensitive nature of the information that may be gleaned from that data, the mere retention of such data by providers of electronic communications services entails a risk of abuse and unlawful access.”

⁶⁸⁴ Nettesheim, 2015: 61. The author explores this issue in the following paragraphs. It is beyond the scope of this work, but he raises relevant questions for future data retention systems. Nettesheim goes on to argue that the “Court did not enquire whether statistical evidence would support the assumption that a sufficient number of people have indeed developed the ‘vague feeling of surveillance’ since the transposition of the Directive into national laws, and it did also not aspire to establish whether electronic communication was indeed affected by the requirements of the Directive...Looking into the future, the question will be whether the Court will continue to apply this rather subjective concept (relating to possible feelings of the communicating persons), if popular conceptions about what data are typically or legitimately stored in a communication process are changing. In developing its normative standard, the Court relies heavily on the current notions of a certain group of (mostly older) European citizens — notions that have emerged largely in the 20th century. It might well be that we are witnessing the emergence of a new generation of information technology users who will be aware of, and will be willing to accept a communication environment, which is characterized by much more data gathering than we are used to today (or are at least aware of today)...I am not joyfully anticipating an era, in which the collection of data by service providers and ‘objects’ (the Internet of things) will be the standard, but looking at the development of the last 20 years, the emergence of such a cultural environment is anything but improbable. The jury is still out determining whether the judgment of the Court will contribute to the establishment of new standards, or whether it will be washed away by an unstoppable technological and cultural tide.”

⁶⁸⁵ Joined cases C-293/12 and C-594/12, paragraph 36.

⁶⁸⁶ Article 1(1) of Directive 2006/24/EC.

As such, it had to comply with Article 8 CFREU. The judges explained their reasoning by saying that the:

[R]etention of data for the purpose of possible access to them by the competent national authorities, as provided for by Directive 2006/24, directly and specifically...falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, therefore, necessarily has to satisfy the data protection requirements arising from that article.⁶⁸⁷

The retention of data is part and parcel of processing operations. It is where they begin. So, regulating retention sufficed to make the provisions of the Directive fall under that rule of the CFREU. Since it also regulated access to data by law enforcement so that they could investigate, detect, and prosecute crime,⁶⁸⁸ no doubts remained for the Court that the Directive provided for an interference with the fundamental right to data protection.

1.1.2 When did the interference take place?

The interference occurred at two moments. First, when providers retained data. And, secondly, when law enforcement agencies accessed such information.⁶⁸⁹ Each processing stage seems to present a potential interference.

1.1.3 Was the interference serious?

AG Cruz Villalón said the interference was especially serious.⁶⁹⁰ While the Directive forbade the retention of the content of communications, it nevertheless created a system to retain vast amounts of information related to daily telecommunications in massive databases.⁶⁹¹ For him, this could make EU citizens feel they were under a constant risk of surveillance during the data retention period.⁶⁹² The Directive required:

⁶⁸⁷ Joined cases C-293/12 and C-594/12, paragraph 29.

⁶⁸⁸ Article 1(1) of Directive 2006/24/EC.

⁶⁸⁹ Joined cases C-293/12 and C-594/12, paragraphs 35 and 36. The Court leaned on the jurisprudence of the ECtHR to sustain this, namely cases *Leander v Sweden*, 26 March 1987 (9248/81), paragraph 48, *Rotaru v Romania*, 4 May 2000 (28341/95), paragraph 46 (which mentions the referred case *Amann v Switzerland*, paragraphs 69 and 80, and *Kopp v Switzerland*, 25 March 1998 (23224/94), paragraph 53), and *Weber and Saravia v Germany*, 29 June 2006 (54934/00), paragraph 79.

⁶⁹⁰ Opinion of AG Cruz Villalón, paragraph 70.

⁶⁹¹ *Idem*, paragraphs 71 and 72.

⁶⁹² *Idem*, paragraph 72.

[T]he retention of every piece of communications data generated by every person in every Member State of the European Union, irrespective of whether or not individuals were suspected of any wrongdoing and notwithstanding that national law might recognise certain communications to be privileged. The duty to retain data was not subject to any restriction, exception or limitation.⁶⁹³

The AG felt this to be particularly grave since the impact of such interference was amplified by the relevance of telecommunications in contemporary times. Their extensive and widespread use by most EU citizens in their professional and personal lives⁶⁹⁴ had the capacity to turn the data retention Directive into a pervasive method for controlling data and people, whose effects were hidden behind a veil of ignorance.⁶⁹⁵ This idea of control has been further explored by Andrew Roberts. He considers that:

The acquisition of data might facilitate more subtle forms of interference. If we can draw inferences about a subject's interests, strategies, fears and weaknesses, we can devise counterstrategies, manipulate and nudge him in the direction of choices we think more desirable...This kind of manipulation depends on the subject being unaware that [he] has suffered a loss of privacy and that information acquired as a consequence of the loss is being used to ensure that [he] decides in accordance with the manipulators' preferences rather than [his] own. Awareness leaves open the possibility of resistance.⁶⁹⁶

Directive 2006/24/EC was, undeniably, supposed to work under a veil of secrecy as data subjects were not to be regularly informed about processing undertakings. As a result, compelling the retention of those data was virtually arbitrary.

The CJEU thus found the interference to privacy and data protection rights caused by that Directive to be extensive and exceptionally serious.⁶⁹⁷ Such information could allow law enforcement to draw inferences about “the number and nature of a person's relationships; the state of his finances; his political views, religion, sexual orientation, life plans and other aspirations; what opinions he might hold about others; his fears, predilections and foibles.”⁶⁹⁸

As Andrew Roberts concluded, the seriousness of the interference was due to the fact that telephone and internet metadata can expose more about one individual than what those closest to him know. This should suffice to make individuals watchful when limiting their freedoms in such an apparently voluntary way. Plus, there were no reasonable exceptions to prevent the

⁶⁹³ Roberts, 2015: 541.

⁶⁹⁴ Opinion of AG Cruz Villalón, paragraph 73.

⁶⁹⁵ Roberts, 2015: 544.

⁶⁹⁶ *Idem*: 545.

⁶⁹⁷ Joined cases C-293/12 and C-594/12, paragraph 37.

⁶⁹⁸ Roberts, 2015: 544.

retention of communications data, like professional or trade confidentiality.⁶⁹⁹ As Tuomas Ojanen incisively commented, this type of general and rather intrusive surveillance scheme has a detrimental influence on the bond between governments and citizens.⁷⁰⁰

The Court followed the opinion of the AG. It argued that, as data were collected and processed without the service user knowing, this would give rise to a reasonable fear that peoples' lives were under continuous monitoring.⁷⁰¹

The judges afterwards explored the criteria stemming from Article 52(1) CFREU.⁷⁰² According to that norm, any "limitation on the exercise of the rights and freedoms laid down by the Charter"⁷⁰³ must: i) be provided for by law; ii) respect the essence of the affected rights and freedoms; iii) serve purposes of general interest recognized by the EU; and iv) under the principle of proportionality, be necessary and limited to that which is strictly necessary.⁷⁰⁴ These criteria are cumulative, meaning that failing to comply with one is enough for the Court to conclude that the interference violates the CFREU.⁷⁰⁵

1.2 Provided for by law

The first criterion was not addressed by the Court. The interference was provided for by law as this was a preliminary ruling on the validity of the provisions of a Directive, an act giving rise to legal effects contained in EU secondary law. From a formal point of view, Article 52(1) CFREU was satisfied in this regard.⁷⁰⁶

⁶⁹⁹ Stoeva, 2014: 582.

⁷⁰⁰ Ojanen, 2014: 536.

⁷⁰¹ Joined cases C-293/12 and C-594/12, paragraph 37. Following the words of Fennelly, 2019: 681, it is interesting to note the variation in language used in the case law as compared to that used by AG Cruz Villalón. While the CJEU talked about a "feeling that their private lives [were] the subject of constant surveillance," the AG had used a softer tone by referring to a "vague feeling of surveillance...which implementation of Directive 2006/24 may cause" (paragraph 52). The Court would maintain this tone in subsequent case law, namely joined cases C-203/15 and C-698/15, paragraph 100.

⁷⁰² Andrew Roberts thinks there is a lack of answers in the CJEU's jurisprudence on the interests that privacy serves (Roberts, 2015: 542). Based on Möller, 2014, Roberts suspects that the principle of proportionality might not suffice to understand the seriousness of the interference caused by the data retention Directive upon this right.

⁷⁰³ Article 52(1) CFREU.

⁷⁰⁴ Joined cases C-293/12 and C-594/12, paragraph 38.

⁷⁰⁵ Ojanen, 2014: 533.

⁷⁰⁶ Opinion of AG Cruz Villalón, paragraph 108.

1.3 The essence of the rights

1.3.1 To privacy

The judges found that the data retention Directive did not allow access to content data, which led them to conclude that the essence of privacy remained intact.⁷⁰⁷ Article 1(2) expressly stated that, despite applying to “traffic and location data on both legal entities and natural persons [it did not] apply to the content of electronic communications, including information consulted using an electronic communications network.”⁷⁰⁸

Some literature has criticized this position. Already in 2014, Tuomas Ojanen saw this as the easy way out, pointing out the fact that:

[T]he distinction between the content of the electronic communications and...metadata as traffic data and location data is rapidly fading away in a modern network environment. A lot of information, including sensitive information, about an individual can easily be revealed by monitoring the use of communications services...Hence, the processing of metadata cannot any longer be invariably seen as falling within such ‘peripheral areas’ of privacy and data protection where limitations would be permissible much more easily than in the context of the content of electronic communications. Indeed, the more systematic and wide the collection, retention and analysis of metadata becomes, the closer it can be seen as moving towards the core area of privacy and data protection with the outcome that at least the most massive, systematic forms of collection and analysis of metadata can be regarded as constituting an intrusion into the inviolable core of privacy and data protection.⁷⁰⁹

Xavier Tracol also found the opinion of the Court problematic, since a systematic assessment of online and telephone metadata allows authorities to glean substantial intelligence on data subjects, which clearly encroaches upon the essence of privacy.⁷¹⁰ This is, truly, an outdated distinction between content data and metadata. The judges ignored the fact that modern big data systems can provoke a particularly serious interference with privacy just by using metadata.

⁷⁰⁷ Joined cases C-293/12 and C-594/12, paragraph 39. See also joined cases C-203/15 and C-698/15, paragraph 101.

⁷⁰⁸ Article 1(2) of Directive 2006/24/EC.

⁷⁰⁹ Ojanen, 2014: 537.

⁷¹⁰ Tracol, 2014: 741.

1.3.2 To data protection

Similarly, the CJEU believed that the essence of data protection was respected. Article 7 of Directive 2006/24/EC imposed “certain principles of data protection and data security [upon] providers.”⁷¹¹ They aimed at maintaining the quality of data (Article 7(a)), as well as securing their physical integrity (b). They also ensured limited access by competent authorized personnel (c) and their elimination upon the expiry of the retention period (d).

This position again provoked disagreement in the literature. Maria Porcedda said that the CJEU found the essence of this right to lie in respecting minimal data security protections.⁷¹² Her opinion echoes that of Tzanou, who criticized the limited way in which the judges viewed this right, reducing it to the principle of data security and excluding aspects like transparency or the right to information, which are an integral part of the right to data protection.⁷¹³

The problem was clearly explained by Orla Lynskey, when arguing that the:

Court envisag[ing] that technical data security concerns lie at the heart of this newly recognized right...is likely to divide opinion. It is unexpected insofar as such data security measures are not explicitly mentioned in the wording of Article 8 of the EU Charter. [W]hile Article 8...does not explicitly refer to data security or ‘technical and organizational principles’, the Article is titled ‘Protection of Personal Data’ and such principles provide the practical means to protect personal data. The Court is therefore perhaps suggesting that the essence of the right to data protection is not an *objective* of that right...but rather it is the *means* of achieving data protection that constitutes the essence of the right.⁷¹⁴

It is questionable that the Directive, as well as other big data-based systems, do not interfere with the essence of the fundamental rights to privacy and to data protection. This also raises the question of whether a proportionality test was actually necessary in this case, in light of what has been said on the cumulative nature of the criteria set out in Article 52 CFREU.

1.4 Objectives of general interest recognized by the EU

The Court considered that the retention of telecommunications data satisfied an objective of general interest recognized by the Union. The substantive goal of the data retention Directive

⁷¹¹ Article 7 of Directive 2006/24/EC.

⁷¹² Porcedda, 2018: 306.

⁷¹³ Tzanou, 2017: 60.

⁷¹⁴ Lynskey, 2015: 172.

was to guarantee that collected information was accessible for law enforcement purposes, thereby helping to counter crime and ensure public security.⁷¹⁵

Fighting cross border terrorism and serious crime to keep peace and security in the EU has been generally recognized as an objective of general interest in the CJEU's case law.⁷¹⁶ As such, retaining personal data to allow national agencies to access and use them in preventing and countering crime, especially of a complex nature, indisputably satisfies this requirement.⁷¹⁷

1.5 The principle of proportionality

The last step was to assess whether the interference was appropriate and necessary to achieve the purposes of the legislation.⁷¹⁸ As Alessandro Spina put it, this ruling came:

[I]n a line of cases in which the ECJ has given weighty recognition to the fundamental rights of privacy and data protection in the legal order of the EU and [upheld] the principle that proportionality is the paramount principle in the judicial

⁷¹⁵ Joined cases C-293/12 and C-594/12, paragraph 41. The CJEU did not address proportionality in relation to what the AG apparently considered the main purpose of the Directive, that of ensuring the general performance of the Union's internal market (Opinion of AG Cruz Villalón, paragraphs 100 ff.).

⁷¹⁶ The Court alluded to joined cases C-402/05 P and C-415/05 P, *Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities*, 3 September 2008 (ECLI:EU:C:2008:461), paragraph 363, C-145/09, paragraphs 46 and 47, and C-539/10 P and C-550/10 P, *Stichting Al-Aqsa v Council of the European Union and Kingdom of the Netherlands v Stichting Al-Aqsa*, 15 November 2012 (ECLI:EU:C:2012:711), paragraph 130.

⁷¹⁷ Joined cases C-293/12 and C-594/12, paragraphs 43 and 44.

⁷¹⁸ *Idem*, paragraph 46. Using the principle of proportionality, one of the general principles of EU law, is a judicial practice well consolidated at EU and national level. The Court referred to settled jurisprudence to back this claim, namely cases C-343/09, *Afton Chemical Limited v Secretary of State for Transport*, 8 July 2010 (ECLI:EU:C:2010:419), paragraph 45 (which mentions cases C-189/01, *H. Jippes, Afdeling Groningen van de Nederlandse Vereniging tot Bescherming van Dieren and Afdeling Assen en omstreken van de Nederlandse Vereniging tot Bescherming van Dieren v Minister van Landbouw, Natuurbeheer en Visserij*, 12 July 2001 (ECLI:EU:C:2001:420), paragraph 81, C-558/07, *The Queen, on the application of S.P.C.M. SA, C.H. Erbslöh KG, Lake Chemicals and Minerals Ltd and Hercules Inc. v Secretary of State for the Environment, Food and Rural Affairs*, 7 July 2009 (ECLI:EU:C:2009:430), paragraph 41, and C-379/08 and C-380/08, *Raffinerie Mediterranée (ERG) SpA, Polimeri Europa SpA and Syndial SpA v Ministero dello Sviluppo economico and Others (C-379/08) and ENI SpA v Ministero Ambiente e Tutela del Territorio e del Mare and Others (C-380/08)*, 9 March 2010 (ECLI:EU:C:2010:127), paragraph 86), C-92/09 and C-93/09, *Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen*, 9 November 2010 (ECLI:EU:C:2010:662), paragraph 74 (which mentions case C-58/08, *The Queen, on the application of Vodafone Ltd and Others v Secretary of State for Business, Enterprise and Regulatory Reform*, 8 June 2010 (ECLI:EU:C:2010:321), paragraph 51), C-581/10 and C-629/10, *Emeka Nelson and Others v Deutsche Lufthansa AG and TUI Travel plc and Others v Civil Aviation Authority*, 23 October 2012 (ECLI:EU:C:2012:657), paragraph 71 (which mentions joined cases C-27/00 and C-122/00, *The Queen v Secretary of State for the Environment, Transport and the Regions, ex parte Omega Air Ltd (C-27/00) and Omega Air Ltd, Aero Engines Ireland Ltd and Omega Aviation Services Ltd v Irish Aviation Authority (C-122/00)*, 12 March 2002 (ECLI:EU:C:2002:161), paragraph 62, and C-504/04, *Agrarproduktion Staebelow GmbH v Landrat des Landkreises Bad Doberan*, 12 January 2006 (ECLI:EU:C:2006:30), paragraph 35), C-283/11, *Sky Österreich GmbH v Österreichischer Rundfunk*, 22 January 2013 (ECLI:EU:C:2013:28), paragraph 50, and C-101/12, *Herbert Schaible v Land Baden-Württemberg*, 17 October 2013 (ECLI:EU:C:2013:661), paragraph 29. All the cases mentioned refer to other case law, which demonstrates that using the principle of proportionality is a well-established practice.

review of measures providing interferences into the private life of individuals as provided in the judgment *Rundfunk*.⁷¹⁹

The Court stressed that the EU legislator had limited discretion to approve measures interfering to such a serious extent with fundamental rights and that it would assess such discretion very rigorously.⁷²⁰ As the Council of the EU would later recognize, the CJEU showed that it would not be satisfied with anything other than a thorough examination of the adequacy and necessity of serious interferences to fundamental rights, regardless how valid the intentions of the EU legislator might be.⁷²¹

The judges did not rule out the validity of retaining personal data on a large scale to fight terrorism and complex crime. Still, if the EU decides to do this, it has an obligation to provide for stringent measures to protect rights and freedoms. The collection and processing of metadata and content data cannot be, as Arianna Vidaschi says, widespread or arbitrary.⁷²² As such, the Court first assesses the adequacy and then the strict necessity of EU secondary law. The next sections will expound these two standards, as the judges did in their ruling.

1.5.1 Adequacy

The first part of the proportionality test was deemed by the Court to have been met. The adequacy criterion implies that any measure or policy must be fit to attain its purposes.⁷²³ The Directive provided supplementary tools to national law enforcement units to deal with serious crime.⁷²⁴ In light of the increasing use of online and telecommunications, retaining communications data was seen as appropriate⁷²⁵ to achieve those purposes.

Data may, indeed, be an essential help to counter crime. While not all means of communication were targeted, the CJEU decided that this did not make the Directive inappropriate, or devoid of purpose.⁷²⁶ This was a limitation by design⁷²⁷ which, if anything, rendered it more in line with fundamental rights.

⁷¹⁹ Spina, 2014: 250. The author was referring to joined cases C-465/00, C-138/01 and C-139/01.

⁷²⁰ Joined cases C-293/12 and C-594/12, paragraphs 47 and 48.

⁷²¹ Information Note (9009/14, 5.5.2014), paragraph 19.

⁷²² Vidaschi, 2019: 278.

⁷²³ Borriello, 2020: 160.

⁷²⁴ Joined cases C-293/12 and C-594/12, paragraph 49.

⁷²⁵ The CJEU used the word ‘appropriate’ as synonym for ‘adequate’ in its jurisprudence. They will be used interchangeably here as well.

⁷²⁶ This was what Mrs. Tschohl and Seitlinger, as well as the Portuguese Government, had considered in their written observations to defend the inadequacy of the Directive.

⁷²⁷ Joined cases C-293/12 and C-594/12, paragraph 50.

1.5.2 Strict necessity

The case was not so linear regarding strict necessity. This second criterion of the principle of proportionality requires that the measure or policy to be implemented only interferes with the life and rights of the affected individuals strictly as much as is truly necessary. It should be as least intrusive as possible.⁷²⁸ The Council of the EU commented that legislation encroaching upon fundamental rights:

[D]o not stand a serious chance of passing the legality test unless they are accompanied by adequate safeguards in order to ensure that any serious restriction of fundamental rights is circumscribed to what is strictly necessary and is decided in the framework of guarantees forming part of Union legislation instead of being left to the legislation of Member States.⁷²⁹

The CJEU agreed that, in principle, the success of the fight against terrorism and serious crime, as well as of any measures guaranteeing public security, is based, to a large degree, on advanced investigative methods.⁷³⁰ However, from the different techniques available, the retention and processing foreseen by the legislator in the Directive seemed excessive as judged by the standards of the purposes it pursued.

Besides, the judges were concerned that the virtual world may present additional risks that make it harder to justify retaining personal data online. In fact, under this Directive, data were to be automatically processed.⁷³¹ Although it failed to deepen its reasoning, the Court felt that this presented a substantial risk that such information could be accessed illegally.⁷³² Perhaps it meant that having data circulate in virtual channels increases the risk of exposure, compared to storing them only in a physical format.

It is relevant to recall that the Court addressed privacy and data protection rights in an intertwined way. This was particularly evident in the assessment of strict necessity. It argued that, to protect private life, interferences with the safety of data must be limited to what is

⁷²⁸ Borriello, 2020: 160.

⁷²⁹ Information Note (9009/14, 5.5.2014), paragraph 19.

⁷³⁰ Joined cases C-293/12 and C-594/12, paragraph 51. See also joined cases C-203/15 and C-698/15, paragraph 103.

⁷³¹ *Idem*, paragraph 55. This would be echoed in Opinion 1/15, paragraph 141, and joined cases C-511/18, C-512/18 and C-520/18, paragraph 132.

⁷³² *Ibidem*. The CJEU used previous cases of the ECtHR to illustrate its concerns by analogy, namely *S. and Marper v the United Kingdom*, paragraph 103, and *M. K. v France*, 18 April 2013 (19522/09), paragraph 35 (which mentions case *B.B., Gardel, and M.B. v France*, 17 December 2009 (5335/06, 16428/05, and 22115/06), paragraphs 53, 61, and 62).

strictly necessary.⁷³³ For the CJEU, it seems that only adequate data protection measures can ensure the privacy of consumers whenever their personal data are retained by third parties. This is why it claimed that the right to data protection present in Article 8(1) CFREU is of particular importance to upholding the right to privacy foreseen in Article 7 CFREU.⁷³⁴

The judges were raising awareness of the fact that, as regards telecommunications, privacy can only be preserved through robust schemes that shield personal data and give data subjects relevant and effective data rights. For this reason, they stated that EU law:

[M]ust lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect personal data against the risk of abuse and against any unlawful access and use of that data.⁷³⁵

While it recognizes two different rights, this argument appears to portray data protection as a functional tool serving the preservation of privacy.⁷³⁶ This might be a dangerous precedent for the theoretical foundations of the fundamental right to the protection of personal data.

The next paragraphs explore the aspects of Directive 2006/24/EC that led the Court to consider that it went beyond what was strictly necessary. As stated above, it focuses only on issues that were key to finding the Directive disproportionate and that can be transposed to assess the intra-EU PNR system. They are the quantity of collected data, the length of the retention period, and access rights by third parties.

A. Quantity of collected data

The Court said that the retention of all information relating to telecommunications and online usage of every consumer interfered with the rights of almost all EU citizens.⁷³⁷ It caused a

⁷³³ Joined cases C-293/12 and C-594/12, paragraph 52. The Court again referred to settled case law, namely case C-473/12, *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and Others*, 7 November 2013 (ECLI:EU:C:2013:715), paragraph 39 (which mentions case C-73/07, *Tietosuoja- ja valtuutus- ja Satakunnan Markkinapörssi Oy and Satamedia Oy*, 16 December 2008 (ECLI:EU:C:2008:727), paragraph 56).

⁷³⁴ *Idem*, paragraph 53. In relation to this point applied to a different field of study, see Stoica & Safta, 2015: 97.

⁷³⁵ *Idem*, paragraph 54. See also joined cases C-203/15 and C-698/15, paragraph 109. This was another lesson drawn from the jurisprudence of the ECtHR, namely cases *Liberty and Others v the United Kingdom*, 1 July 2008 (58243/00), paragraphs 62 and 63, *Rotaru v Romania*, paragraphs 57 to 59 (which mention case *Klass and Others v Germany*, 6 September 1978 (5029/71), paragraphs 49 and 50), and *S. and Marper v the United Kingdom*, paragraph 99 (which mentions cases *Kruslin v France*, 24 April 1990 (11801/85), paragraphs 33 and 35, and *Association for European Integration and Human Rights and Ekimdzhiiev v Bulgaria*, 28 June 2007 (62540/00), paragraphs 75 to 77).

⁷³⁶ Marin, 2016: 219.

⁷³⁷ Joined cases C-293/12 and C-594/12, paragraph 56. This resulted from reading together Articles 3, on the obligation to retain data, and 5(1), on the categories of data to be retained, of Directive 2006/24/EC.

“general and indiscriminate”⁷³⁸ interference that made no distinction between individuals, and tabled no restrictions or exceptions, in the fight against complex crime, thereby affecting people with no proof of a connection, either direct or indirect, between their behavior and serious crime.⁷³⁹ As Arianna Vidaschi would later add, the Directive did not distinguish between innocent individuals and criminal suspects. It allowed for the retention of and access to metadata, provided the communications occurred in the EU.⁷⁴⁰

The Directive was found to allow for the retention of excessive data from too many persons. The judges argued that data systems should establish a link between the data and concrete dangers to the public, as well as permitting only the collection of information concerning a specific time, zone, and individuals potentially involved in criminal practices.⁷⁴¹ In fact, data to be collected should be likely to contribute to preventing, detecting, or prosecuting serious crime.⁷⁴² As none of these criteria were present in the Directive, Luisa Marin commented that:

[I]n its reasoning on the scope of the surveillance, the Court rejected the pre-emptive logic which has animated many of the counter-terrorist measures, the logic according to which total surveillance is needed because the fight is targeting an absolute evil. [In] *Digital Rights Ireland*...the Court rejected the necessity of an EU legal instrument derogating from the principles of the constitutional state based on the rule of law [and] the ‘panopticism’ underlying this and other measures adopted in the surveillance package.⁷⁴³

B. Data retention period

Article 6 of the Directive determined that all data should be retained between six and 24 months, irrespective of a connection with any potential added value for its security purposes.⁷⁴⁴ Cruz Villalón stated that keeping data at unspecified online sites should be seen as extraordinary.⁷⁴⁵

⁷³⁸ Case C-623/17, paragraph 80.

⁷³⁹ Joined cases C-293/12 and C-594/12, paragraphs 57 and 58. See also joined cases C-203/15 and C-698/15, paragraphs 105 and 110, C-623/17, paragraphs 77 ff., and C-511/18, C-512/18 and C-520/18, paragraphs 143 and 145. It is important to highlight that, in joined cases C-203/15 and C-698/15, the CJEU was quite firm in adding that, although the “substantive conditions which must be satisfied by national legislation...may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected.”

⁷⁴⁰ Vidaschi, 2019: 276. See also Faull, 2011: 611 ff.

⁷⁴¹ The CJEU reached a similar conclusion in joined cases C-203/15 and C-698/15, paragraph 107, and C-511/18, C-512/18 and C-520/18, paragraphs 141 and 144.

⁷⁴² Joined cases C-293/12 and C-594/12, paragraph 59. See also joined cases C-203/15 and C-698/15, paragraph 106.

⁷⁴³ Marin, 2016: 219.

⁷⁴⁴ Joined cases C-293/12 and C-594/12, paragraph 63.

⁷⁴⁵ Opinion of AG Cruz Villalón, paragraph 144.

The collection of personal data should not be seen as a regular practice. It should, instead, be perceived as an exception limited in time to that which is strictly necessary. After discussing the differences between present and historical time, he concluded that data should be retained for no more than a year.⁷⁴⁶ Only exceptional reasons⁷⁴⁷ could justify longer periods.

Curiously, the CJEU identified two different problems. It did not discuss the length of the retention period but, instead, challenged the fact that the definition of the exact period of retention in each member state did not depend upon common objective criteria which could limit it to what was necessary.⁷⁴⁸ Some literature has endorsed this opinion and explored the scarce arguments of the Court. Stoeva, for instance, has said that the absence of a common data retention period could warp or influence the competition in the EU's internal market of telecommunications providers. It could result in a lack of legal certainty, with providers having to modify their business every time they wanted to operate in different member states and with consumers being unsure of how long their data would actually be kept in their databases.⁷⁴⁹

The second problem was that there were no guarantees that, at the expiry of the retention period, data would be deleted permanently.⁷⁵⁰ The CJEU thus concluded that the Directive did not interfere in a limited way with the rights foreseen in Articles 7 and 8 CFREU.⁷⁵¹

C. Third parties with access rights

C.1 Public entities

Article 4 of the Directive contained a formula that gave a wide margin of discretion to member states in terms of access to data. It stated that:

Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or

⁷⁴⁶ Opinion of AG Cruz Villalón, paragraph 149.

⁷⁴⁷ *Idem*, paragraph 151.

⁷⁴⁸ Joined cases C-293/12 and C-594/12, paragraph 64.

⁷⁴⁹ Stoeva, 2014: 584.

⁷⁵⁰ Joined cases C-293/12 and C-594/12, paragraph 67.

⁷⁵¹ *Idem*, paragraph 65.

public international law, and in particular the ECHR as interpreted by the European Court of Human Rights.⁷⁵²

There were many problems there. The Court argued that access by data processors should be limited. It found that there were no clear limits on accessing and processing data, and that the Directive failed to set out objective standards against which such limits could be defined.⁷⁵³ In particular, the judges thought it was crucial that any operation performed upon the data was limited to the goals of the Directive and served to fight only clearly specified crimes. The conclusion was that the legislator had been careless by not detailing the material and formal criteria for processing operations.⁷⁵⁴

Member states had to respect the “relevant provisions of European Union law or public international law.”⁷⁵⁵ However, it seems the CJEU suspected national legislatures would not keep such standards. It is not clear why the Court suspected this, but it may have just wanted to ensure an *ex ante* protection, at the level of EU law.

Cruz Villalón made a similar remark in his Opinion. He wrote that the:

European Union legislature cannot, when adopting an act imposing obligations which constitute serious interference with the fundamental rights of citizens of the Union, entirely leave to the Member States the task of defining the guarantees capable of justifying that interference. It cannot content itself either with assigning the task of defining and establishing those guarantees to the competent legislative and/or administrative authorities of the Member States called upon, where appropriate, to adopt national measures implementing such an act or with relying entirely on the judicial authorities responsible for reviewing its practical application. It must...fully assume its share of responsibility by defining at the very least the principles which must govern the definition, establishment, application and review of observance of those guarantees.⁷⁵⁶

This means that EU secondary law must create common obligations for member states on access to data that limit it according to what is necessary, namely by providing a framework of the conditions for private actors to allow public entities access to their collected material, or for private actors to send them such data.⁷⁵⁷ This tables legislative safeguards to ensure the Union’s values and principles are preserved and that citizens have their privacy protected against abusive big data retention schemes.

⁷⁵² Article 4 of Directive 2006/24/EC.

⁷⁵³ Joined cases C-293/12 and C-594/12, paragraph 60.

⁷⁵⁴ *Idem*, paragraph 61.

⁷⁵⁵ Article 4 of Directive 2006/24/EC.

⁷⁵⁶ Opinion of AG Cruz Villalón, paragraph 120.

⁷⁵⁷ Joined cases C-203/15 and C-698/15, paragraphs 117 and 118.

The Court concluded by mentioning other features which the data retention Directive should have incorporated to satisfy the necessity principle from the perspective of access to data.⁷⁵⁸ It should have set concrete conditions to allow for the identification of individuals with access rights, and of those who could process and handle data, limiting such rights to what would be necessary. Moreover, it should have included a mechanism of *ex ante* review by a judicial or independent body that would seek to monitor access to data by those who require it.⁷⁵⁹ An alternative would be to contain an explicit obligation for member states to legislate on this.

As these criteria were absent from the Directive, the CJEU determined that the Union legislator had gone beyond the conditions of the proportionality principle, in light of Articles 7, 8, and 52(1) CFREU. The Directive was invalid as it stood.⁷⁶⁰

C.2 Private actors

The Directive was also flawed due to the data security arrangements applied during processing by providers of telecommunications services. This was the only time the Court talked about an interference exclusively to do with data protection. It noted concerns on the level of protection guaranteed, and about the fact that processing operations could be undertaken overseas.

C.2.1 Level of protection

The CJEU began by saying that the Directive failed to reach the standard of protection of Article 8 CFREU, because it did not contain the necessary measures to effectively protect the information against the possibility of misuse or unauthorized access and processing by private

⁷⁵⁸ The CJEU did not discuss the silence of the Directive regarding access conditions. Still, the AG had admitted that it was the “very regulation of the conditions for access and use of the collected and stored data which [made] it possible to assess the scope of what that interference entail[ed] in practical terms and which may, therefore, determine whether or not the interference [was] constitutionally acceptable” (Opinion of AG Cruz Villalón, paragraph 121). This was the case because of the “intimate relationship between the specific configuration of the obligation to collect and retain data and the circumstances in which those data [were], where appropriate, made available to the competent national authorities and used by them” (paragraph 122).

⁷⁵⁹ Joined cases C-293/12 and C-594/12, paragraph 62. See also Opinion of AG Cruz Villalón, paragraph 131, where he took the view that “Directive 2006/24 [was] as a whole incompatible with Article 52(1) of the Charter, since the limitations...to retain data which it [imposed were] not accompanied by the necessary principles...needed to regulate access to the data and their use,” and joined cases C-203/15 and C-698/15, paragraphs 120 (which mentions ECtHR case *Szabó and Vissy v Hungary*, 12 January 2016 (37138/14), paragraphs 77 and 80) and 123 (which mentions case C-362/14, paragraphs 41 and 58).

⁷⁶⁰ *Idem*, paragraphs 69, 71, and 73. This same conclusion had been adopted by the AG, who claimed that Directive 2006/24/EC was in direct conflict with Article 52(1) CFREU (paragraph 159).

providers. Similarly to its treatment of access by public entities, the Court then listed the concrete issues which the legislation should have addressed. In its view:

Article 7 of Directive 2006/24 [should have laid] down rules which [were] specific and adapted to (i) the vast quantity of data whose retention [was] required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.⁷⁶¹

In short, the Directive did not guarantee that all providers would apply a high standard of data protection and security through technological and operational adaptation.⁷⁶² It seems that, for the judges, the legislation should have established common rules that would compel private actors to adapt their operations, systems, and general functioning, in order to keep data safe while they were collected and processed. Or, at least, it should have contained norms instructing member states to make providers act accordingly.

Beyond that, a high level of data protection was also jeopardized because its Article 7 allowed providers to consider economic factors when setting the level of data security applied in their operations, such as the costs of implementation. The provision was silent on economic considerations. Yet, it stated that compliance with “data security principles with respect to data retained in accordance with [the] Directive [was without] prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC.”⁷⁶³ Articles 4(1) of Directive 2002/58/EC and 17(1), 2nd paragraph, of Directive 95/46/EC held that all appropriate technical and organizational measures to protect personal data should observe the “state of the art and the cost of their implementation.”⁷⁶⁴

As Directive 2006/24/EC did not expressly dismiss these economic considerations, the Court reasoned that Article 7 allowed providers to circumvent the obligation to implement adequate security mechanisms. This is rather convoluted reasoning, but it has the merit of seeking to prevent member states and private actors from implementing more relaxed data safeguards, especially considering that security protocols might be expensive to keep in big data systems.

⁷⁶¹ Joined cases C-293/12 and C-594/12, paragraph 66. See also joined cases C-203/15 and C-698/15, paragraph 122.

⁷⁶² *Idem*, paragraph 67.

⁷⁶³ Article 7 of Directive 2006/24/EC.

⁷⁶⁴ Articles 4(1) of Directive 2002/58/EC and 17(1), 2nd paragraph, of Directive 95/46/EC.

C.2.2 Processing overseas

Finally, the judges likewise found it problematic that data processing activities could take place outside the Union. Cruz Villalón had raised awareness of this by pointing out that the Directive did not require service providers to store data within the borders and jurisdiction of the member states.⁷⁶⁵ This sort of “outsourcing” of data retention admittedly allow[ed] the retained data to be distanced from the public authorities of the Member States and thus to be placed beyond their direct grip and any control.”⁷⁶⁶

The CJEU concurred with his reasoning. It claimed that if data could be retained beyond EU borders, it would be difficult, or even impossible, to guarantee oversight by independent administrative authorities of whether the provisions on data protection and security were being respected, as necessary under Article 8(3) CFREU.⁷⁶⁷

With these last remarks, the Court wanted to buttress the idea that keeping data safe in big data retention schemes is not an obligation imposed solely on law enforcement and public authorities. Private actors also have a key role to play in protecting data whenever they are involved in their processing. Even if they previously accessed that same data in the course of their business without applying high data protection guarantees, the adding of a public security purpose changes the rationale for data safety.⁷⁶⁸

1.6 Relevant takeaways

The key findings of this ruling are as pertinent today as they were in 2014. If anything, the entry into force of the GDPR has reinforced the need to make big data retention systems exceptional and watertight with regard to the privacy and safety of the personal information of data subjects. The EU legislator must refrain from approving legislation that allows for the collection of big troves of data from service users. It should, instead, opt for systems that retain and process selected pieces of information in relation to targeted individuals, and even such targeted processing has to be justified by objective criteria. Besides, data can only be kept for a limited

⁷⁶⁵ Opinion of AG Cruz Villalón, paragraph 78.

⁷⁶⁶ *Idem*, paragraph 79. It is curious to note that, while the AG was trying to demonstrate how this outsourcing endangered privacy, the CJEU focused its reasoning on data protection.

⁷⁶⁷ Joined cases C-293/12 and C-594/12, paragraph 68. This legal and geographic concern can already be found in case C-614/10, *European Commission v Republic of Austria*, 16 October 2012 (ECLI:EU:C:2012:631), paragraph 37 (which mentions case C-518/07, *European Commission v Federal Republic of Germany*, 9 March 2010 (ECLI:EU:C:2010:125), paragraph 23).

⁷⁶⁸ Joined cases C-293/12 and C-594/12, paragraph 66.

time and their use for law enforcement purposes must depend on prior review by courts or other independent bodies.

The small-step approach taken by the Court in this case law has been very useful in identifying the key elements that should be included when assessing the proportionality of big data retention systems. From the analysis, it becomes clear that the data retention Directive seriously interfered with the fundamental rights to privacy and to data protection. This interference, however, was provided for by law and served objectives of general interest recognized by the Union. For the judges, it also managed to keep the essence of these rights intact. This is not consensual and, if they had found differently, it would have been sufficient to declare the Directive invalid with no need for further developments. In any case, the CJEU found that such interference was adequate to achieve the objectives of the legislation, but was not limited to that which is strictly necessary to do so. The Directive was therefore considered invalid for its violation of key rights enshrined in the CFREU.

Analyzing Digital Rights Ireland, nevertheless, leads us to wanting more from the CJEU. It has been too brief in developing some of its arguments, leaving open questions that weaken their strength. The Court's lack of engagement with the essence of the rights to privacy and data protection is striking, for example. To find that the essence of these rights is kept intact because only metadata are retained falls short as an argument, given the potential for non-content data to interfere with private life, traceability, and the identification of natural persons.

2. Opinion 1/15

The following pages will assess Opinion 1/15 in much the same way as the previous section analyzed joined cases C-293/12 and C-594/12. It will be seen that the main issues identified regarding Digital Rights Ireland also arise in relation to the PNR Agreement with Canada, showing that the Union still has a long way to go when it comes to conceiving and drafting big data retention systems. The Agreement was not capable of guaranteeing the level of protection needed to ensure protection for the fundamental rights of passengers. Perhaps the day will come when the Court will assess the PNR agreements struck with Australia and the US and likewise find that they are disproportionate.

On 25 June 2014, the Commission signed an Agreement with Canada for the transfer of API and PNR data from European air passengers. It then requested approval by the Council and the EP. On 25 November, the latter requested an opinion from the CJEU on its compatibility with

primary law, namely Articles 16 TFEU and 7, 8, and 52(1) CFREU, and concerning specifically the right to data protection.⁷⁶⁹

The Agreement served to provide a sort of adequacy decision for transferring PNR.⁷⁷⁰ Protecting data was, apparently, one of its key purposes.⁷⁷¹ However, the EP argued that, globally considered, the system could permit law enforcement to gather very specific details on the private activities of passengers.⁷⁷²

The EP added that the Agreement should have imposed minimum protections to ensure that data were safe from misuse or unauthorized access.⁷⁷³ Similar concerns were present in *Digital Rights Ireland*,⁷⁷⁴ as well in case law of the ECtHR.⁷⁷⁵ AG Mengozzi made similar observations, recalling that any EU law provision requiring the processing of personal information leads to a violation of the right to data protection, as established in Article 8 CFREU.⁷⁷⁶

On 26 July 2017, the Court issued what Mengozzi⁷⁷⁷ and some authors consider to be its first decision on whether international agreements are compatible with the CFREU.⁷⁷⁸ The Agreement was found to be incompatible with primary law and the judges drew a roadmap explaining what should be changed to make it valid. As Brendan Lord put it, PNR systems can comply with treaty law and fundamental principles only if they are designed with concrete scopes and truly abide by data protection norms.⁷⁷⁹

The discussion will proceed as follows. In accordance with the case law, this section first identifies the interferences with the rights to privacy and data protection. It then questions whether such interferences have been provided for by law, encroach upon the essence of those rights, and serve objectives of general interest recognized by the Union. The following

⁷⁶⁹ Opinion 1/15, paragraph 1.

⁷⁷⁰ *Idem*, paragraph 31. Its Article 5 read that “[s]ubject to compliance with this Agreement, the Canadian Competent Authority [was] deemed to provide an adequate level of protection, within the meaning of relevant European Union data protection law, for the processing and use of PNR data. An air carrier that provides PNR data to Canada under this Agreement [was] deemed to comply with European Union legal requirements for PNR data transfer from the European Union to Canada.”

⁷⁷¹ *Idem*, paragraph 33.

⁷⁷² *Idem*, paragraphs 35 and 36. These same concerns appear in the initial paragraphs of *Digital Rights Ireland*. See also joined cases C-293/12 and C-594/12, paragraph 27.

⁷⁷³ *Idem*, paragraph 39.

⁷⁷⁴ Joined cases C-293/12 and C-594/12, paragraph 54.

⁷⁷⁵ *Case Liberty and Others v the United Kingdom*, paragraphs 62 and 63.

⁷⁷⁶ Opinion of AG Mengozzi, paragraph 171.

⁷⁷⁷ *Idem*, paragraph 7.

⁷⁷⁸ Kuner, 2018: 858. See also Hijmans, 2017: 409, and Zalnieriute, 2018: 1054, who added that “[i]n light of the data protection trilogy in *Digital Rights Ireland-Schrems-Tele2 Sverige*...an adverse CJEU opinion on the proposed EU-Canada PNR agreement hardly comes as a surprise. *Opinion 1/15* was entirely consistent with the recent post-Snowden case-law, however, it also went further and elaborated more detailed requirements for the transfers of personal data to third countries and for the first time ruled on the compatibility of a draft international agreement with the fundamental rights under the Charter.”

⁷⁷⁹ Lord, 2019: 265.

subsections apply proportionality tests to such interferences, assessing their compliance with the criteria of adequacy and strict necessity. There is a final subsection on the right to notification of air passengers, which the CJEU discussed beyond the proportionality test.

2.1 Serious interference

First, the Court considered whether the PNR Agreement gave rise to a serious interference with fundamental rights. It claimed that the collection and handling of EU PNR receipts by Canada and transfers to other third countries interfered with the fundamental right to privacy foreseen in Article 7 CFREU.⁷⁸⁰ It further added that the right to data protection, enshrined in Article 8, was likewise affected because such operations came down to data processing.⁷⁸¹ As in joined cases C-293/12 and C-594/12, the judges made no distinction between privacy and data protection, which is consistent with the Court's propensity to assess these rights together.⁷⁸²

As mentioned above, this is not the most suitable way to protect such rights. The decision to assess them together here was due to constraints of space and time. It is without prejudice to the criticism that such an approach can weaken the strength of any judicial reasoning.

2.1.1 Was there an interference?

The Court began by saying that PNR are data from identified or identifiable passengers.⁷⁸³ According to established case law,⁷⁸⁴ using such information can seriously interfere with private life and the security of personal data;⁷⁸⁵ with 'using' referring to all operations regarding data.

As such, sharing data with third parties certainly interferes with privacy and data protection, regardless what happens to the information afterwards. This reasoning applies when those parties are public agencies and even when data subjects have not been concretely bothered as a result of the intrusion.⁷⁸⁶

⁷⁸⁰ Opinion 1/15, paragraph 125.

⁷⁸¹ *Idem*, paragraph 126. The Court made here reference to case C-543/09, *Deutsche Telekom AG v Bundesrepublik Deutschland*, 5 May 2011 (ECLI:EU:C:2011:279), paragraph 52.

⁷⁸² Kuner, 2018: 873. See also Docksey, 2016: 200, Lynskey, 2014: 1807 ff., and Woods, 2017.

⁷⁸³ Opinion 1/15, paragraph 122.

⁷⁸⁴ See joined cases C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) v Administración del Estado*, 24 November 2011 (ECLI:EU:C:2011:777), paragraph 42, and C-291/12, *Michael Schwarz v Stadt Bochum*, 17 October 2013 (ECLI:EU:C:2013:670), paragraph 26.

⁷⁸⁵ Opinion 1/15, paragraph 122.

⁷⁸⁶ *Idem*, paragraphs 124 and 126. The Court referred here to case C-362/14, paragraph 87.

2.1.2 When did the interference take place?

The Agreement was found to provoke several interferences with fundamental rights. This was, again, an echo of previous case law.⁷⁸⁷ It was also a response to the claim of the United Kingdom that all or most of the passengers impacted by the Agreement would not be inconvenienced by the interference.⁷⁸⁸ The CJEU was very precise in this respect, claiming that all use “permitted, inter alia, by Articles 3, 4, 6, 8, 12, 15, 16, 18 and 19 of the envisaged agreement, constitute[d] interferences with the right guaranteed in Article 7 of the Charter.”⁷⁸⁹

Additionally, again, the Court found that it likewise affected the fundamental right to data protection because this was also a matter of data processing.⁷⁹⁰ The discomfort of the judges is already palpable here in relation to this system of data retention. This became even clearer when they commented that the intrinsic features of the PNR regime set out in the Agreement testify to the true nature of the interferences.⁷⁹¹

2.1.3 Was the interference serious?

The CJEU illustrated its previous argument by reference to features through which the seriousness of the interferences stood out. A first example was the fact that data of all travelers were to be systematically and continuously transferred to Canada.⁷⁹² Data were to be processed electronically in a similar fashion prior to arrival, cross-checking them with different databases according to pre-determined templates and requirements.⁷⁹³

Combining systematic transfers with systematic processing could have a significant impact on the lives of passengers. Data might expose all the details of a flight itinerary, as well as travel patterns, associations between travelers, and even sensitive elements like economic statuses or eating and health conditions.⁷⁹⁴ They could also lead to other discoveries since PNR aims to reveal previously unknown facts and hidden links. Air passengers hereafter became suspects.⁷⁹⁵

Automatic processing might subject air passengers to programmed decisions that could have

⁷⁸⁷ Joined cases C-293/12 and C-594/12, paragraph 33.

⁷⁸⁸ Opinion of AG Mengozzi, paragraph 172.

⁷⁸⁹ Opinion 1/15, paragraph 125.

⁷⁹⁰ *Idem*, paragraph 126.

⁷⁹¹ *Idem*, paragraph 129.

⁷⁹² *Idem*, paragraph 127.

⁷⁹³ *Idem*, paragraph 131.

⁷⁹⁴ *Idem*, paragraph 128.

⁷⁹⁵ Opinion of AG Mengozzi, paragraph 176.

serious consequences.⁷⁹⁶ The risk is that these decisions could be taken without concrete facts to sufficiently support the conclusion that the affected individuals pose a threat to public security. The Court feared that Canadian security personnel could make biased inferences, i.e., inferences not based on serious security risks.

This shows that the interferences were deemed to be serious, and that the Agreement failed to guarantee a fundamentally similar protection to that provided in the EU.⁷⁹⁷ Some scholars have found this position excessive. Romain Tinière believes the CJEU did not seem to want an equivalent protection but that “les autorités canadiennes appliquent pleinement le droit de l’Union relatif à la protection des données à caractère personnel.”⁷⁹⁸

The judges then assessed whether these interferences were justified and proportionate. They first recalled that the rights to privacy and data protection can have their scope limited, according to Article 52 CFREU.⁷⁹⁹

Christopher Kuner and other scholars have seen here a positive development in that the judges backed down from banning completely the possibility of retaining data on a large scale, thus recognizing that interferences with the fundamental rights to privacy and data protection may be acceptable, in certain cases, to pursue general security objectives recognized by the Union.⁸⁰⁰ This is a reference to when the Court said that:

[W]hile the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight.⁸⁰¹

This was a position originally laid down in joined cases C-293/12 and C-594/12. In those cases, the judges had claimed that, no matter how important the fight against serious crime might be, it did not render the data retention mechanisms foreseen in Directive 2006/24/EC necessary to achieve such a purpose.⁸⁰² The problem was that this gave little margin of

⁷⁹⁶ Opinion 1/15, paragraph 132.

⁷⁹⁷ *Idem*, paragraph 134.

⁷⁹⁸ Tinière, 2018.

⁷⁹⁹ Opinion 1/15, paragraph 136. The AG had said that they are not an “absolute prerogative” (Opinion of AG Mengozzi, paragraph 181). The CJEU mentioned case C-112/00, *Eugen Schmidberger, Internationale Transporte und Planzüge v Republik Österreich*, 12 June 2003 (ECLI:EU:C:2003:333), paragraph 80.

⁸⁰⁰ Kuner, 2017.

⁸⁰¹ Joined cases C-203/15 and C-698/15, paragraph 103.

⁸⁰² *Idem*, paragraph 51.

discretion for the EU legislator to draft policies that, though based on the collection and processing of big data, could be justified.

The following pages review the criteria used by the CJEU to assess the interferences provoked by the PNR Agreement. The judges discussed whether they were provided for by law, respected the essence of individual rights, and were limited to what was strictly necessary.⁸⁰³

2.2 Provided for by law

Contrary to the EP,⁸⁰⁴ the judges argued that Article 218(6) TFEU, on the conclusion of agreements adopted by the Council, mirrors, externally, the separation of powers that exists, internally, among the EU institutions. It imitates the procedure for approving internal policies and applies it to the adoption of international agreements.⁸⁰⁵

AG Mengozzi had previously commented that, provided the PNR Agreement was sanctioned by the EP and then adopted by the Council, it would become part and parcel of the Union's legal order. For him, there was little doubt as to whether the interference it provoked was provided for by law.⁸⁰⁶ The CJEU concurred, saying that "such an agreement may be regarded as being the equivalent, externally, of that which is a legislative act internally."⁸⁰⁷

2.3 The essence of the rights

2.3.1 To privacy

The Court found that the essence of privacy was respected. It was argued that, even if PNR receipts could, on certain occasions, disclose rather concrete aspects about the privacy of data subjects, that information only concerned some aspects of their lives, namely to do with their flights between the EU and Canada.⁸⁰⁸

⁸⁰³ Opinion 1/15, paragraphs 138 ff.

⁸⁰⁴ *Idem*, paragraph 145.

⁸⁰⁵ *Idem*, paragraph 146.

⁸⁰⁶ Opinion of AG Mengozzi, paragraph 192.

⁸⁰⁷ Opinion 1/15, paragraph 146.

⁸⁰⁸ *Idem*, paragraph 150. Following the comments of Lenaerts, 2012: 391, it appears that the CJEU has seldom found the essence of fundamental rights to be violated in data retention schemes. As Tambou, 2018: 194, claimed, "*Opinion 1/15* confirmed the cautious application of the concept of the essence of the fundamental rights by the ECJ. So far, regarding surveillance, the ECJ has concluded only once, in the *Schrems* case, that the essence of the right of privacy and the right of judicial review was affected. The interference with the essence of the fundamental right to privacy was due to the access, on a generalized basis, to the contents of electronic communication of data subjects by the American public authorities." In fact, in case C-326/14, paragraph 94, it can be read that "[i]n

2.3.2 To data protection

The CJEU reached the same conclusion regarding the essence of data protection. Maria Porcedda argues that it found the Agreement to respect the essence of this right because its Article 3 limited the purposes of processing by Canada⁸⁰⁹ and Article 9 laid down rules to keep data secure.⁸¹⁰ Still, Maria Tzanou disagrees and contends that:

The blanket collection of the PNR data of every passenger, irrespective of whether he is considered to be under suspicion, its retention for long periods and its processing in order to develop terrorist profiles, without granting adequate procedural rights to the individuals concerned to challenge it, affects cumulatively the essence of several different fair information principles and, might, therefore, be considered to touch upon the essence of the fundamental right to data protection.⁸¹¹

Lorna Woods is also hesitant in this matter. She reasons that, in Opinion 1/15 as much as in joined cases C-293/12 and C-594/12, it is not possible to grasp the essence of this right for the CJEU. It seems that, regardless of the amount of information collected and how exhaustive profiling can be, the essence of data protection remains unharmed. She concedes that a narrow view of the essence of rights like privacy and data protection is plausible. Yet, the judges should explain what they think that essence is, and if it is the same for Articles 7 and 8 CFREU.⁸¹² This is a significant point. We would learn a great deal about the reasoning of the Court if indeed it were to answer these questions.

2.4 Objectives of general interest recognized by the EU

The legal basis was seen by the Court as a matter inextricably linked to the issue of identifying whether the purpose of the Agreement was an objective of general interest recognized by the Union.⁸¹³ This posed little controversy as the purpose of the Agreement was to counter terrorism and cross-border crime, thus guaranteeing security more broadly. This is clearly an objective

particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.”

⁸⁰⁹ Porcedda, 2018: 299.

⁸¹⁰ Opinion 1/15, paragraph 150.

⁸¹¹ Tzanou, 2017: 173.

⁸¹² Woods, 2017.

⁸¹³ Opinion 1/15, paragraph 147. The section on the essence of the rights appears before that on the objectives of general interest recognized by the EU, to follow the same pattern used in joined cases C-293/12 and C-594/12. The CJEU has here changed the order of the analysis, but this has no relevant impact on the general appraisal of the Agreement.

of general interest that suffices to warrant serious interferences with fundamental rights.⁸¹⁴

Brendan Lord argued that it could even be seen to pursue another objective explicit in the Charter. PNR contributes to individual security,⁸¹⁵ protected in Article 6 CFREU. This system does, indeed, serve more than just the interests of public security. This will not be explored further, however, as it is a discussion beyond the scope of this research.

2.5 The principle of proportionality

Monika Zalnieriute claims that the limitations of the Agreement surfaced⁸¹⁶ when assessing the aptness of the system's processing operations in relation to the purpose of maintaining public security.⁸¹⁷ She also highlighted another important aspect, which has already been mentioned. The CJEU was so detailed in its analysis that this jurisprudence could explain "how *any* PNR agreements should be drafted to ensure their compatibility 'with the treaties and with the constitutional principles stemming therefrom.'"⁸¹⁸ This is an interesting remark as it points to the growing awareness of the Court as to the details of big data retention schemes, but also as it confirms that Opinion 1/15 has been a good choice to study in depth in order to assess the intra-EU PNR system. The conclusions of the CJEU serve to judge international agreements as much as internal legislation.

2.5.1 Adequacy

Compliance with the first component of proportionality was swiftly verified. It may be helpful to recall that this requires that any given measure must be appropriate to achieve its objectives. The Court began by alluding to a document issued by the Commission in 2010,⁸¹⁹ in which it had argued that assessing data before the arrival of passengers to Canada served to fight crime and to expedite security checks and border control.⁸²⁰

Still, Opinion 1/15 also mentions reports from local authorities indicating that only 178 persons were arrested from 28 million passengers assessed between April 2014 and March

⁸¹⁴ Opinion 1/15, paragraphs 148 and 149.

⁸¹⁵ Lord, 2019: 264.

⁸¹⁶ Zalnieriute, 2018: 1052.

⁸¹⁷ Opinion 1/15, paragraphs 152 ff.

⁸¹⁸ Zalnieriute, 2018: 1053.

⁸¹⁹ Communication (COM(2010) 492 final, 21.9.2010), section 2.2.

⁸²⁰ Opinion 1/15, paragraphs 152 and 153.

2015.⁸²¹ It seems quite unclear on what basis the CJEU found this system adequate.

The judges may have set a risky precedent by not considering the efficacy of a policy that results in so few detentions after so many persons have been screened. It is unclear whether it is PNR which is adequate to deter criminals and terrorists, or API and the previously existing security tools. In fact, a measure such as this “must not just have some logical link to its intended objective, but should also be «effective» at achieving it. A measure which is...demonstrably grossly ineffective in achieving it, cannot ever be said to be «appropriate».”⁸²² Olivia Tambou rightly claims that the numbers mentioned above are not persuasive regarding the added value of sending PNR information in bulk to Canada. The Court should have criticized the lack of impact assessments, and better developed its stance on the adequacy of the Agreement.⁸²³

2.5.2 Strict necessity

Despite this, the Court carried on with its proportionality analysis, checking whether the interferences were restricted to the strictly necessary and whether the PNR Agreement defined its data protection norms in a clear way.⁸²⁴ For AG Mengozzi, the idea was to check if the Union and Canada had found the right equilibrium between the purpose of fighting crime and terrorism, and the requirement to keep data and privacy safe.⁸²⁵

As with Directive 2006/24/EC, the key features discussed here were the quantity (and, this time, also the quality) of collected data, the data retention period, and access rights by third parties. The CJEU tackled other aspects which will not be considered as they are less relevant to the analysis of the intra-EU PNR scheme.⁸²⁶ In any case, we see positive developments in the case law as a result of the Opinion given that the Court provided more detail in scrutinizing the Agreement as compared to the data retention Directive, not least to ensure the maintenance of a high level of protection for fundamental rights.

A. Quantity and quality of collected data

Data retention systems should be sufficiently precise to enable the identification of the material

⁸²¹ Opinion 1/15, paragraph 152.

⁸²² Electronic Frontier Foundation, 2014: 20.

⁸²³ Tambou, 2018: 196.

⁸²⁴ Opinion 1/15, paragraph 154.

⁸²⁵ Opinion of AG Mengozzi, paragraph 207.

⁸²⁶ Some examples of these other aspects are the automated processing of data, secondary purposes for using PNR, disclosure to individuals, redress, and oversight of data protection safeguards.

undergoing processing. Besides this, they should guarantee that sensitive data are not collected, or are duly protected. The Court said that the Agreement should specify in a clear and complete way which data carriers should be expected to send to Canada.⁸²⁷

A.1 A matter of quantity

Mengozi remarked that some headings of the Annex to the Agreement were written in such a broad way that even a fairly educated passenger would not be capable of knowing all the data elements that could be included in those headings.⁸²⁸ The Annex listed the elements that carriers should transfer to Canadian authorities and he was thinking of headings 5, 7, and 17. The Court would concur with his argument, claiming that these entries were vague and imprecise.⁸²⁹

Heading 5 mentioned “available frequent flyer and benefit information,”⁸³⁰ specifying, in brackets, that this meant free tickets, upgrades, and “etc.”⁸³¹ The problem was with this last term, which opened the range of information that could be included. It also left a broad margin for interpretation as to whether it covered data relating simply to the rank of passengers in customer programs, or everything that concerned flights and transactions undertaken by those passengers under such programs.⁸³²

Similarly, heading 7 asked carriers to transfer “[a]ll available contact information.”⁸³³ This made it hard to know what contact data should be included in receipts, namely whether they should contain data of people other than the passenger, like those who had booked the ticket or emergency contacts.⁸³⁴

Finally, heading 17 was deemed a “free text heading”⁸³⁵ since it allowed for the adding of “general remarks”⁸³⁶ to the PNR receipts. It set no limitations on what could be used or collected, falling short in terms of transparency and accuracy. In fact, it opened the possibility of including data completely irrelevant to the security goals of the transfers.⁸³⁷

Both the AG and the Court concluded that the extent of the interference of headings 5, 7, and 17 with privacy and data protection was not limited to the strictly necessary in terms of

⁸²⁷ Opinion 1/15, paragraph 155.

⁸²⁸ Opinion of AG Mengozzi, paragraph 207.

⁸²⁹ Opinion 1/15, paragraph 156.

⁸³⁰ Heading 5 of the Annex of Agreement (12657/5/13 REV 5, 23.6.2014).

⁸³¹ *Idem*.

⁸³² Opinion 1/15, paragraph 157.

⁸³³ Heading 7 of the Annex of Agreement (12657/5/13 REV 5, 23.6.2014).

⁸³⁴ Opinion 1/15, paragraph 158.

⁸³⁵ *Idem*, paragraph 160.

⁸³⁶ Heading 17 of the Annex of Agreement (12657/5/13 REV 5, 23.6.2014).

⁸³⁷ Opinion 1/15, paragraph 160.

transparency and precision.⁸³⁸ AG Mengozzi added that to make those categories and the material scope of the Agreement compliant with strict necessity, carriers and Canadian law enforcement could not have a margin of discretion to define the extent of the categories of data to be retained.⁸³⁹

A.2 A matter of quality

The quantity and quality of data are naturally related. If heading 17 allowed unknown data to be included in PNR receipts, sensitive data could end up being included there as well. Moreover, if Articles 8, on the use of such data, and 16, on their retention, of the Agreement tabled concrete norms on the processing of sensitive material, this obviously meant that both Canada and the EU had agreed that such data could be sent to the former.⁸⁴⁰ Mengozzi had referred to this problem when pointing out that the Agreement left space for details on the health, ethnicity, or religion of air passengers to be revealed.⁸⁴¹

The Court positively stressed that any decision taken on the basis of sensitive data and in spite of the particular behavior of the passengers would violate the fundamental rights foreseen in Articles 7 and 8 CFREU.⁸⁴² This should be interpreted together with Article 21 CFREU, which lists the data whose processing might lead to negative discrimination.

So, the judges concluded that, for sensitive data to be transferred to third countries, there should have to be a strong and concrete reason. It would not be sufficient to generally claim the defense of public security against terrorist and serious criminal acts. As this was not the case in the PNR Agreement, they held that the transfers, handling, and processing of sensitive material foreseen therein were in violation of Articles 7, 8, and 21 CFREU.⁸⁴³

Vedaschi sees here a positive note that the CJEU did not entirely close the door to special circumstances. This does not appear to be a case of outright prohibition but, instead, of a general rule with very concrete exceptions.⁸⁴⁴ Alas, the Court did not elaborate further and this is not a consensual matter. For Hijmans, for example, this opening is in conflict with the Court's views on the processing of sensitive data and raises questions about the limits of the essence of

⁸³⁸ Opinion 1/15, paragraph 163. See also Opinion of AG Mengozzi, paragraph 225.

⁸³⁹ Opinion of AG Mengozzi, paragraph 220.

⁸⁴⁰ Opinion 1/15, paragraph 164.

⁸⁴¹ Opinion of AG Mengozzi, paragraph 221.

⁸⁴² Opinion 1/15, paragraph 165.

⁸⁴³ *Idem*, paragraph 167.

⁸⁴⁴ Vedaschi, 2018: 422.

privacy, whose breach is by itself unlawful and excluded from proportionality assessments.⁸⁴⁵

The practical consequence of allowing for the processing of sensitive data in unknown situations is the risk of vast numbers of passengers being stigmatized, even though they are not suspects of any crime. This prompted the AG to advise the Court to declare unlawful the inclusion of any sensitive data within the scope of the Agreement.⁸⁴⁶ He recalled that Article 8 of the PNR Agreement with Australia prohibits any “processing by the Australian Customs and Border Protection Service of sensitive PNR data.”⁸⁴⁷ If the use of sensitive data is prohibited in another international agreement, then the purpose of fighting serious crime and terrorism is achievable with similar efficacy, without sensitive data having to be transferred to Canada.⁸⁴⁸ The judges maintained the opening to transfers of sensitive material in certain circumstances, despite the warnings of the AG. Time will tell whether it is a sensible option.

B. Data retention period

The Commission and the Council sustained that the estimated lifetime of transnational criminal webs, as well as the intricacy and length of criminal investigations, required a long data retention period and that data needed to be kept after passengers departed from Canada.⁸⁴⁹ The CJEU concurred with this point regarding the length of the data retention period, saying that:

[I]t must nevertheless be accepted, in the light, *inter alia*, of the considerations put forward, in particular, by the Council and the Commission...that the five-year retention period provided for in Article 16(1) of that agreement [did] not exceed the limits of what [was] strictly necessary for the purposes of combating terrorism and serious transnational crime.⁸⁵⁰

Yet, it added that, if passengers did not present a risk until departure, and after going through airport security, there would be no link between their personal information and the purposes of the Agreement to sustain the retention of data after they left Canada.⁸⁵¹ This is an important point⁸⁵² that may impact future data retention policies. Data of innocent EU citizens should not be retained by third countries after passengers leave them. Therefore, keeping their information

⁸⁴⁵ Hijmans, 2017: 410 and 411.

⁸⁴⁶ Opinion of AG Mengozzi, paragraph 222.

⁸⁴⁷ Article 8 of Agreement (OJ L 186, 14.7.2012).

⁸⁴⁸ Opinion of AG Mengozzi, paragraph 222.

⁸⁴⁹ Opinion 1/15, paragraph 205.

⁸⁵⁰ *Idem*, paragraph 209.

⁸⁵¹ *Idem*, paragraph 205.

⁸⁵² Vidaschi, 2018: 424.

after they left Canada so that law enforcement authorities could access such data despite the absence of any connection with the purposes of the PNR Agreement was found unlawful and unjustified.⁸⁵³ Nor was it considered limited to what was necessary.⁸⁵⁴ The Court maintained that data could only be stored when PNR enabled authorities to infer that determined passengers might pose a threat to public security even after they had left the country.⁸⁵⁵

It is up for discussion whether the Court should have criticized the lengthy retention period foreseen in the Agreement. It is, however, understandable that it did not. It appears that the judges did not feel empowered to ascertain whether five years is too long to allow law enforcement to keep data for complex criminal investigations. They decided that that was a task for the legislator, together with experts. This is also why the CJEU only passed judgment on those aspects of the temporal element that were clearly unnecessary, i.e., the use of data of passengers with no clear criminal connections after they left Canada.

Mengozi made additional remarks that can be quite useful in assessing data retention systems. He believed that data could be retained for long periods after departure, provided that there was a sufficient, concrete rationale.⁸⁵⁶ His prime contention was with the retention of all types of PNR data without differentiation. The AG questioned:

[W]hether, after several years, there is justification for retaining certain categories of data...In particular, [he] wonder[ed] whether frequent flyer and benefit information...information about the check-in status...ticketing or ticket price information...and code sharing information...which, according to the Commission, provide information only about the actual carrier prove...to be information having genuine added value by comparison with the other data which [are] also retained and which may be unmasked, with the aim of combating terrorism and serious transnational crime.⁸⁵⁷

In keeping with this line of thought, he condemned Article 16(3) of the Agreement for providing for the depersonalization of only certain data. It allowed relevant elements to remain unmasked, such as payment and frequent flyer data.⁸⁵⁸

⁸⁵³ Opinion 1/15, paragraph 205.

⁸⁵⁴ *Idem*, paragraphs 206 and 211.

⁸⁵⁵ *Idem*, paragraph 207.

⁸⁵⁶ Opinion of AG Mengozzi, paragraph 279.

⁸⁵⁷ *Idem*, paragraph 284.

⁸⁵⁸ *Idem*, paragraph 287.

C. Third parties with access rights

The Court made two relevant remarks regarding access rights. On the one hand, it argued that the Agreement foresaw no general rule establishing that access to data would be:

[S]ubject to a prior review carried out either by a court, or by an independent administrative body, and that the decision...be made following a reasoned request by the competent authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime.⁸⁵⁹

On the other hand, its Article 19, on the disclosure of data outside Canada, allowed it to transfer PNR to third countries without there being a similar agreement between them and the EU, or an adequacy decision from the Commission endowing the Canadian authorities with access rights and guaranteeing that the country in question would ensure the level of protection required by EU law.⁸⁶⁰ These transfers depended on the discretionary powers of CBSA, which was responsible for assessing the level of data protection guaranteed by other third countries.⁸⁶¹ The Court hence found that provision to go beyond what was necessary.⁸⁶²

AG Mengozzi similarly opposed the fact that data could be transferred at the discretion of that agency without a prior review by a judicial or independent body.⁸⁶³ In his view, any *ex post* control would be beyond the actual competence and review powers of the judicial courts and authorities of the third country in question.⁸⁶⁴ The risk of bypassing EU law standards of data protection was, therefore, quite real.⁸⁶⁵

2.6 Right to notification

This additional subsection of the analysis of Opinion 1/15 is included here because the CJEU did not tackle individual data rights within its assessment of the proportionality of the PNR Agreement. However, this part raises key points which are too significant to be overlooked. It must also be noted that data rights were only discussed in Opinion 1/15 and not in the earlier Digital Rights Ireland case. This issue is likewise addressed in more recent jurisprudence, which

⁸⁵⁹ Opinion 1/15, paragraph 202.

⁸⁶⁰ *Idem*, paragraph 214.

⁸⁶¹ Kuner, 2018: 872.

⁸⁶² Opinion 1/15, paragraph 215.

⁸⁶³ Opinion of AG Mengozzi, paragraph 300.

⁸⁶⁴ *Idem*, paragraph 302.

⁸⁶⁵ *Idem*, paragraph 305.

reinforces the claim that the case law is evolving. The Court is learning to address policies based on the retention of big data and it is sharpening its approach to fundamental rights in the context of modern technologies.

In this regard, the judges considered that the exercise of individual data rights and the processing of data in a legally sound way depend on a robust system of notification,⁸⁶⁶ as well as the supervision of independent authorities and the possibility of redress. Only the first aspect will be developed here because the intra-EU PNR system contains a mechanism for independent supervision.⁸⁶⁷ Plus, the CJEU found that Article 14 of the Agreement contained sufficient administrative and judicial mechanisms of redress.⁸⁶⁸

By contrast, the exercise of data rights was not guaranteed in the Agreement as it did not foresee an individual notification procedure which would apply when the Canadian competent authorities used PNR. This obligation was not present in Articles 12, on access rights, or 13, on the right to correction of data. Nor could it be found in Article 11, which instructed Canada to make available, on the website of its competent authority, general information on the processing and exchange of PNR.⁸⁶⁹

Article 11 did not oblige Canada to tell passengers whether their personal information had been accessed for reasons other than security and border control by its competent authorities. This requirement, that there be an individual notification system in place, may prove instrumental in changing the design of data retention systems. The Court set an important standard here, reinforcing it in later cases.⁸⁷⁰ It stressed that access to data should, as a general principle, depend on the individual notification of affected passengers, and on prior review by a judicial or independent administrative authority.

This makes the use of PNR data beyond security checks dependent upon three criteria: i) a reasoned request based on concrete proof to justify access;⁸⁷¹ ii) prior authorization issued by a court or independent body; and iii) that competent authorities notify each affected air passenger.

⁸⁶⁶ Opinion 1/15, paragraph 219. See also joined cases C-511/18, C-512/18 and C-520/18, paragraph 190.

⁸⁶⁷ See Articles 6(7), 13(5), (6), and (8), and 15, together with recitals (32) and (37), of Directive (EU) 2016/681.

⁸⁶⁸ Opinion 1/15, paragraph 227. In Opinion of AG Mengozzi, paragraph 320, the AG shared a partially different view, noting that there was “no reference in the agreement envisaged to the existence of...administrative appeal to the Canadian Privacy Commissioner.” As such, it seemed it did not expressly foresee for an “independent supervisory authority...to assume directly the task of responding to any request for access, correction or annotation submitted by an individual not present in Canada.” As Article 14(1) of Agreement (12657/5/13 REV 5, 23.6.2014) did not state this clearly, Mengozzi considered the judicial mechanisms of redress were adequate, but the administrative ones were not.

⁸⁶⁹ Opinion 1/15, paragraph 222.

⁸⁷⁰ See, inter alia, joined cases C-203/15 and C-698/15, paragraph 121.

⁸⁷¹ Opinion 1/15, paragraph 223.

Individual notification and prior request and review are cumulative requirements that must be met for law enforcement to make use of passengers' data for investigative purposes. They have become key guarantees of fundamental rights. And the Court has added that these criteria apply whenever data are transmitted to any governmental authority, as well as to individuals and private actors.

There are only two exceptions worth stressing. The first is an exception to prior request and review. If passengers are stopped at security checks in airports based on inferences made from data collected before arrival (or even prior departure), there is no need to ask for authorization from a court or independent administrative body. There is a legitimate expectation from local authorities that passengers consent to their data being analyzed during such procedures. Individuals are aware and are informed of them, even before flying, and this is acceptable provided they can exercise their rights with transparency and legal certainty.

The second is an exception to individual notification. The CJEU emphasized that air passengers must not be notified if that could jeopardize ongoing investigations.⁸⁷² This caveat aims at ensuring that passengers do not tamper with evidence, alter their behavior, or act in any manner that could defeat the investigative purposes.

In the jurisprudence discussed in this chapter, the Court has clarified the rules of the game. The general principle is that any access to PNR information by law enforcement authorities must be clearly limited and justified.⁸⁷³ Only by ensuring respect for these criteria can other data rights be fully respected.

As the PNR Agreement failed to meet these requirements, especially the notification procedures,⁸⁷⁴ it did not live up to the standards set by the CJEU. This will be a crucial finding to use in assessing other data retention schemes. As Elena Carpanelli and Nicole Lazzerini put it, Opinion 1/15 is a landmark in the development of the intra-EU PNR framework.⁸⁷⁵ It opens the way for the invalidation of Directive (EU) 2016/681.

⁸⁷² Opinion 1/15, paragraph 224.

⁸⁷³ *Idem*, paragraph 225.

⁸⁷⁴ Article 9(3) enshrined such obligation only whenever there was unauthorized access or disclosure of information. It was the only provision to mention this, and it read that “[i]f an individual’s PNR data [were] accessed or disclosed without authorization, Canada [should] take measures to notify that individual, to mitigate the risk of harm, and to take remedial action.”

⁸⁷⁵ Carpanelli & Lazzerini, 2017: 401 and 402.

2.7 Relevant takeaways

As with Digital Rights Ireland, there are key takeaways from Opinion 1/15 that will be critical in assessing the validity of the intra-EU PNR. The final part of this chapter tables a legal analysis that is grounded in the arguments put forward by the CJEU, as well as the contributions of scholars and commentators in the legislative process.

In fact, the small-step approach taken again by the Court is not only instrumental in grasping the flaws of the PNR Agreement, but also serves to assess with great detail other PNR systems. From the analysis undertaken in these pages, it becomes clear that the EU-Canada Agreement seriously interfered with the rights to privacy and data protection of many European passengers. This interference was found to be provided for by law and to serve objectives of general interest recognized by the EU. For the judges, the Agreement likewise kept the essence of these rights intact. However, the literature has criticized the Court in this regard, claiming that the essence of data protection, as enshrined in Article 8 CFREU, was breached by the provisions of the Agreement. In any event, the CJEU has found that the interference was adequate to achieve its criminal law purposes, but that the Agreement was disproportionate since it was not limited to that which is strictly necessary to pursue such objectives. The judges thus suggested a long list of changes that should be made to the text of the Agreement so that it could be in line with the fundamental rights and the level of data protection enshrined in EU law.

Opinion 1/15 is sure to have a profound impact on PNR systems in Europe, both in the internal market and in the EU's external relations. It is robust, detailed, and incisive in many regards. It has even been considered an exercise in judicial activism by some scholars. Regardless of being judicial activism or not, it is certainly a critical ruling. The Court has found many flaws that render the Agreement unlawful. It makes it clear that even legislation that aims at fighting crime must do so with full respect for the fundamental rights of all air passengers, through targeted and intelligent law enforcement operations. And this is something the PNR Agreement did not deliver on.

This Agreement allowed for the collection of undetermined data, even opening the door for the retention of sensitive data. As with the data retention Directive, it permitted authorities to collect big troves of material from all air passengers, creating a blanket retention scheme and not a targeted system. Data of innocent passengers were to be kept long after they had departed from Canada, PNR receipts could be sent to third countries without sufficient guarantees of their safety and integrity, and there was no mechanism for prior review, thereby limiting access to data by law enforcement bodies. Besides, the Agreement did not foresee notification

procedures that would allow passengers to know when their data were being processed and to enforce their data rights where necessary.

Despite the clear warnings of the CJEU, the legislator committed many of the same mistakes inherent in the data retention Directive and the PNR Agreement with Canada, in the intra-EU PNR system. The main findings of these two parts of the chapter will now be explored in depth, to support the claim that Directive (EU) 2016/681 should be declared invalid by the Court. In light of the case law discussed here, it is at any rate surprising that it was even approved in the first place.

Chapter 3.3

Trumping fundamental rights: Arrival

“One obvious and distinctive feature that hypocrites seem to share is a kind of mismatch between their pronouncements and their actions. The hypocrite, we tend to think, is someone who says one thing but does another. Yet this cannot be the whole story. Mismatches between our words and our actions are common enough; most of us are occasionally inconsistent...We...argue that hypocrites...*have, by mismatch between judgments and actions, undermined their claim to moral authority...a status that is intimately tied up with their capacity to (1) warrant esteem, and (2) bestow (dis)esteem on others.*”⁸⁷⁶

Introduction

This is the last part of the second thematic chapter. It flows from the previous two parts to make a doctrinal claim regarding the validity of Directive (EU) 2016/681. It argues that, with the approval of PNR, the Union legislator enacted secondary law that fails to protect air passengers’ fundamental rights to privacy and data protection, as well as their individual data rights.

As Hielke Hijmans points out, this legislation was stalled in the EP for quite some time due to its effects on privacy and data protection. Yet, the terrorist events in 2015 in Paris were the trigger which brought it back to the top of the political agenda, and it was adopted shortly after.⁸⁷⁷ Fear and haste are dangerous ingredients in a legislative process, potentially leading legislators to pass laws that breach basic principles. This chapter argues that this happened with the intra-EU PNR, whose published version copies a 2011 proposal which never managed to gain approval due to its ostensible disregard for fundamental rights.

This third part argues that the PNR Directive should be declared invalid due to its incompatibility with the CFREU, if a reference for a preliminary ruling is referred to the CJEU on this question. This position has been advanced by authors like Sylvie Peyrou. In a rather perceptive analysis, following the ruling on joined cases C-293/12 and C-594/12, she revealed an expectation that “[l]’arrêt *Digital Rights Ireland* pouvait laisser espérer une invalidation du système PNR, de par la condamnation que la Cour y prononce de tout stockage de données de masse, et ce de façon indifférenciée.”⁸⁷⁸

Although not all provisions actually encroach upon the norms and legal principles enshrined in primary law, the complexity of PNR and the breadth of its problems should lead the CJEU

⁸⁷⁶ Isserow & Klein, 2017: 191 and 193.

⁸⁷⁷ Hijmans, 2017: 409.

⁸⁷⁸ Peyrou, 2017.

to invalidate it in its entirety. It is not common for the Court to declare an act of EU law fully invalid on its merits.⁸⁷⁹ Yet, Elitsa Stoeva recalls that this has happened precisely with the data retention Directive. This could be one more aspect that Directives 2006/24/EC and (EU) 2016/681 have in common.⁸⁸⁰

This part follows the scheme adopted in the earlier parts of this chapter. No literature has yet analyzed the published version of the Directive in such depth and based on the multifarious sources used here. Some authors suggest that Opinion 1/15 may have a key impact on the intra-EU system⁸⁸¹ but few explore this idea and even fewer do so in detail.⁸⁸² This chapter aims to fill this doctrinal gap.

The legal analysis is based on the sources used before, mainly, but not limited to the two cases of the CJEU studied in depth in the previous part. The recent jurisprudence on the use of telecommunications data for investigation purposes is relevant, in particular, to sharpen the findings of this chapter. However, transposing these cases to PNR has not been taken lightly and the chapter is cautious in this regard.

In fact, the chapter relies heavily on Opinion 1/15 as it is the only PNR case to date. There is still a lack of discussion and clarity about whether the reasoning and findings of the case law on telecommunications data can be transposed to this context. There are arguments in favor of concluding that they can be but there are reasons to be cautious in assuming this as well. On the one hand, the Court is concerned about the general use of personal data for surveillance purposes in telecommunications as well as in other circumstances, like air travel. On the other, there are criteria tabled in the case law that do not seem to adjust well to the logic of PNR and that, therefore, if applied bluntly to the PNR system, would be excessively restrictive and possibly prevent the adaptation of the legislation. As such, as will be discussed in depth below,

⁸⁷⁹ Stoeva, 2014: 590 and 591.

⁸⁸⁰ For Bossong, 2017, “it is almost certain that the EU’s PNR Directive will come next for review before the CJEU, even if the process of implementing the directive and setting up national units in all EU member states for handling PNR data is already underway.”

⁸⁸¹ Zalnieriute, 2018: 1057.

⁸⁸² In an almost anecdotal way, Olivia Tambou succinctly summarizes what she thinks could be distilled from Opinion 1/15 to criticize Directive (EU) 2016/681. She says that “*Opinion 1/15* raise[s] serious concerns about the validity of the PNR Directive...The PNR [d]ata definition present under heading 12 titled ‘general remarks’ could be seen as too vague. The transfer of PNR data to third countries does not refer to the need of an international agreement or a decision of adequacy from the European Commission...Article 13 does not explicitly provide a right to information of the air passenger as required in *Opinion 1/15*. The Directive provide[s] a general five-year retention rule for all PNR data, without consideration whether the person stays or not in the EU territory...It is doubtful that the use of depersonalization technics implemented after six months will be sufficient to consider that this retention regime is limited to what is strictly necessary” (Tambou, 2018: 201). Although she was not focusing on the intra-EU PNR, Tambou addressed the diverse problems she saw in an entire Directive in a single paragraph, at the end of a work on Opinion 1/15. The issue is that this is a common approach of many authors to the EU PNR. They mention it in a tangential manner that leaves more questions than it provides answers. See also Mendez, 2017: 817.

this chapter adopts a cautious reading of the jurisprudence on telecommunications data and criticizes PNR based on standards that clearly stem from Opinion 1/15.

It begins with some notes on the scope and content of the rights to privacy and data protection. It then questions whether PNR seriously interferes with them and if that interference is provided for by law, respects their essence, and serves objectives of general interest recognized by the Union. Following these questions, the analysis moves on to deal with the adequacy and strict necessity of this piece of legislation. This research will conclude by arguing for the invalidity of the Directive in light of the CFREU. A final section additionally discusses the notification procedures embedded in PNR, in a manner similar to the Court in Opinion 1/15.

1. The scope and content of fundamental rights

For reasons of space, as well as to make the claims more robust, the rights to privacy and data protection will be assessed together. This is in line with the case law of the Court and with Article 52(1) CFREU, although the analysis will carefully avoid conflating them, for reasons mentioned earlier, and which will be revisited below. AG Cruz Villalón stressed that any interference with privacy calls for paramount caution⁸⁸³ by the CJEU. Yet, this sort of hierarchy has triggered different reactions.⁸⁸⁴

A common criticism in scholarly writing is that this way of analyzing fundamental rights leads to an unsophisticated and tangential approach to data protection, privileging the right to privacy. This observation is going to be developed in the following sections, together with other aspects regarding the relationship between PNR and these rights. These brief initial sections

⁸⁸³ Opinion of AG Cruz Villalón, paragraphs 58 and 59.

⁸⁸⁴ Maria Tzanou, for example, strongly contests the preeminence given to privacy in works on PNR. From comparing different documents and case law, she believes that data protection, and not privacy, is the key right that lies at the heart of this system. For Tzanou, 2017: 165, “[a]ll the categories of data contained in the PNR constitute information relating to an identified person and, therefore, personal data, regardless of whether they are connected to the intimate private sphere of the person or not. An assessment therefore of [any] PNR case on the basis of the specific data protection principles enshrined in the fundamental right to data protection would not encounter the difficulties found in [an] analysis...carried out on the basis of the right to privacy. But the fundamental right to data protection is not only useful for a finding of interference in the PNR case...The most important contribution of the fundamental right to data protection lies in the assessment of whether the interference posed by PNR is disproportionate or not. Data protection provides for specific principles, on the basis of which such an assessment can be undertaken: among others, purpose limitation, proportionality concerning the amount of data processed and the periods of their retention, consent of the data subject, individual due-process rights, enhanced protection of sensitive data, and independent supervision. It is submitted, therefore, that data protection is the correct fundamental rights basis to assess PNR data transfers for two reasons: first, because all PNR data, despite their level of intimacy, are personal data, and consequently their processing may interfere with the right to data protection if it does not comply with the requirements of Article 8 EUCFR. This approach avoids making fundamental rights protection subject to private law obligations. Second, the specific data protection principles are the right forum to discuss whether such interference is disproportionate, instead of the general privacy right that cannot catch all the problems posed by the PNR transfer.”

serve to provide context before engaging with the proportionality of the interference of PNR with privacy and data protection.

1.1 To privacy

The most pressing issue found by the CJEU in the case law discussed concerned interferences with privacy, as enshrined in Article 7 CFREU. This provision reads that “[e]veryone has the right to respect for his or her private and family life, home and communications.”⁸⁸⁵

The EU legislator did not live up to the expectations enshrined in recital (22) of the PNR Directive. As will be demonstrated, it did not draft a data retention system ensuring “full respect for fundamental rights, for the right to privacy and for the principle of proportionality, [taking] fully into consideration the principles outlined in recent relevant case law of the [CJEU].”⁸⁸⁶ In fact, there is no indication of what jurisprudence was consulted, or if it influenced the legislator.

The drafters were even more daring in recital (36). They wrote that the “Directive respects the fundamental rights and the principles of the Charter, in particular...the right to privacy.”⁸⁸⁷ Stating that it “should therefore be implemented accordingly”⁸⁸⁸ is a hint to member states to transpose the text in line with these apparently high standards. Yet, it will be shown below that the Directive fails to protect privacy in several respects. There is a gap between these recitals and its provisions. As Stoeva commented, already in 2014:

The data retention judgment is strong and unequivocal in asserting that the right to privacy constitutes a fundamental barrier between the individual and powerful institutions, and that laws that allow for blanket retention on this scale are unacceptable. The mass collection of metadata for which the Data Retention Directive was culpable is an unquestionable interference with the right to privacy.⁸⁸⁹

Other authors have invoked similar arguments. Marie-Pierre Granger and Kristina Irion, for instance, believe that the jurisprudence obliges the EU legislator to care for fundamental rights in a more robust manner. They go as far as claiming that it levies a stricter standard for upcoming legislation interfering with personal data.⁸⁹⁰

⁸⁸⁵ Article 7 CFREU.

⁸⁸⁶ Recital (22) of Directive (EU) 2016/681.

⁸⁸⁷ Recital (36) of Directive (EU) 2016/681.

⁸⁸⁸ *Idem*.

⁸⁸⁹ Stoeva, 2014: 591.

⁸⁹⁰ Granger & Irion, 2014: 846.

PNR was, nevertheless, approved without much ado. It appears that the literature and the case law were not sufficiently persuasive for the legislator to avoid creating yet another system based on the blanket retention of big data from large numbers of individuals. The next sections aim to show that policymakers made a poor judgment and the Directive should be invalidated, in a continuation of the saga started in Digital Rights Ireland and continued in Opinion 1/15.

It is important to note that, at the time of writing, there are already pending applications and requests for preliminary rulings challenging its validity.⁸⁹¹ They table interesting ideas and help to reinforce the claim that the Directive is unsuitable as it is. Still, the legal analysis presented here goes beyond the arguments made in these cases.

1.2 To data protection

The other crucial issue discussed by the Court in the jurisprudence analyzed above was the protection of personal data. It comes just after privacy in the Charter, which indicates their theoretical proximity. To recall, Article 8(1) CFREU says that “[e]veryone has the right to the protection of personal data concerning him or her.”⁸⁹² Its following number adds criteria for assessing the legitimacy of interferences with this right, and pinpoints two relevant data rights that are a natural consequence: the rights to access and rectification. It reads that:

Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.⁸⁹³

Additionally, “[c]ompliance with these rules shall be subject to control by an independent authority.”⁸⁹⁴ The CJEU found that this right had been breached in the data retention Directive and in the EU-Canada Agreement. It, nonetheless, ended up using a method of analysis that is, for Ojanen, an approach not likely to satisfy those that have been advocating for the substantive differences between privacy and data protection and, particularly, for the autonomy of the

⁸⁹¹ Beyond the mentioned request for a preliminary ruling in case C-817/19, there are other requests, namely in cases C-215/20, *Bundesrepublik Deutschland*, 19 May 2020, and C-222/20, *Bundesrepublik Deutschland*, 27 May 2020. Moreover, there are recent requests that are still pending applications, namely cases C-148/20, *Deutsche Lufthansa*, 7 August 2020, C-149/20, *Deutsche Lufthansa*, 7 August 2020, C-150/20, *Deutsche Lufthansa*, 7 August 2020, and C-486/20, *Varuh človekovih pravic Republike Slovenije*, 13 November 2020.

⁸⁹² Article 8(1) CFREU.

⁸⁹³ Article 8(2) CFREU.

⁸⁹⁴ Article 8(3) CFREU.

latter.⁸⁹⁵ He was thinking especially of Maria Tzanou,⁸⁹⁶ who wrote a doctoral thesis defending this position at the European University Institute, and on whose examining board Ojanen sat.

In joined cases C-293/12 and C-594/12, the Court considered its claims on privacy applied *mutatis mutandis* regarding data protection.⁸⁹⁷ And, in Opinion 1/15, it said that the operations which might affect privacy could likewise interfere with data protection rights enshrined in Article 8 CFREU, since those operations consist of the processing of personal information.⁸⁹⁸

Some literature has studied this argumentative strategy. It is beyond the scope of the present work, but it is important to argue in favor of having these rights analyzed independently in future decisions. Tzanou is, indeed, one of the most vocal supporters of the relevance of data protection rights. In her view, what is really at stake in PNR systems is this right, and not so much privacy. This is controversial, but she is right in claiming that, considering that data protection has been accepted as an independent right in the jurisprudence of the Court, any position based on the assumption that it has no normative value in itself should be dismissed.⁸⁹⁹

It is true, as Brendan Lord put it, that while these are independent rights, privacy and data protection are inherently connected, since the latter provides the means to exercise one's privacy.⁹⁰⁰ Still, the scope of each extends beyond their areas of overlap. To intertwine them entirely endangers the protection from which individuals may benefit. Juliane Kokott and Christoph Sobotta stress, for instance, that EU secondary data protection laws currently oblige private actors, and not only public authorities, to apply safeguards while processing information. This is a guarantee found under the scope of data protection, not of privacy.⁹⁰¹ As Christopher Docksey remarks:

The CJEU...has erroneously stressed the right of privacy across the board, in cases where personal information was processed but privacy was not necessarily affected. This approach is unnecessary...On the one hand there are cases that do indeed require both rights to be considered because both privacy and data protection are at issue, such as *Digital Rights Ireland* and *Schrems*. In these cases, in addition to the question whether the requirements of the right to data protection have been respected, the processing of personal data constitutes a significant interference with the right of privacy...On the other hand there are cases where there was no interference with privacy and it would have been sufficient to apply the right to data protection. The distinction is important because the analysis of Article 52(1) of the

⁸⁹⁵ Ojanen, 2014: 540.

⁸⁹⁶ The author refers specifically to her thesis on a footnote.

⁸⁹⁷ Joined cases C-293/12 and C-594/12, paragraph 36.

⁸⁹⁸ Opinion 1/15, paragraph 126.

⁸⁹⁹ Tzanou, 2017: 168.

⁹⁰⁰ Lord, 2019: 267.

⁹⁰¹ Kokott & Sobotta, 2013: 225 ff. As they were writing in 2013, the authors were thinking of Directive 95/46/EC. Still, Regulation (EU) 2016/679 and other current secondary laws award even better protection.

Charter applied to the right to privacy looks to justification for an interference, whereas the analysis of Article 52(1) applied to the right to data protection assesses the limitations to the essential elements of the right.⁹⁰²

It is unclear from the case law how data protection is affected independently from privacy. Alessandro Spina remarks that the Court, in joined cases C-293/12 and C-594/12, has found that there is a manifest correlation between these rights which is challenging to untangle.⁹⁰³ And, in fact, such an entwined reasoning can have serious implications if it is to be used to design and assess future data retention schemes.

The CJEU should have developed a robust and autonomous set of arguments to shield data protection per se, as it is a self-standing right in the CFREU. Curiously, it recognized this in joined cases C-203/15 and C-698/15, wherein it remarked that Article 8 CFREU is about a right that is different from the one foreseen in Article 7 CFREU.⁹⁰⁴ These are not only distinct rights, which in itself should preclude their complete overlap; beyond that, assessing data protection often renders discussions about violations of privacy redundant.⁹⁰⁵ Unfortunately, while the judges have recognized that privacy and data protection are separate rights, they have not treated them that way.⁹⁰⁶

To interpret data protection only as a means to ensure the privacy of individuals confines its autonomy, scope, and relevance. This precedent may handicap the theoretical strength of any doctrinal reasoning aimed at protecting it.

2. Serious interference

The first step to assess whether fundamental rights may have been violated by secondary law is to locate the potential interference, as well as to establish its nature and when it can occur. The next subsections will address these matters.

2.1 Is there an interference?

There is an interference with privacy when individual personal data are, or can be, accessed by private or public actors, under provisions of EU law, for security purposes. *À propos* the data

⁹⁰² Docksey, 2016: 201.

⁹⁰³ Spina, 2014: 250.

⁹⁰⁴ Joined cases C-203/15 and C-698/15, paragraph 129, *in fine*.

⁹⁰⁵ Docksey, 2016: 198.

⁹⁰⁶ Lynskey, 2014: 1807.

retention Directive, Elitsa Stoeva argued that processing metadata can expose the personal life of individuals. As such, public bodies with access rights to that kind of information can interfere with their privacy.⁹⁰⁷ If access to metadata meets the threshold for an interference with privacy, giving access to content data is certainly enough to make a similar claim.

In the opening remarks regarding case C-594/12 (Seitlinger and Others) of Digital Rights Ireland, it is mentioned that the Constitutional Court of Austria said that the data retention Directive created a system aiming to store a large number of different types of information from a wide set of people for an extended period of time.⁹⁰⁸ Such a portrayal could be used to depict PNR. It has already been used, in a way, because the Court found, in Opinion 1/15, that the Agreement with Canada entailed extensive and rather serious violations⁹⁰⁹ of Article 7 CFREU.

The CJEU argued that using information from identified, or identifiable, individuals can, indeed, interfere with private life, as foreseen in that provision.⁹¹⁰ The term ‘using’ should be read in broad terms; the mere retention of data, for instance, affects privacy.

On the collection of different types of data, Annex I of Directive (EU) 2016/681 identifies 19 different items of personal information that should be collected by carriers and transferred to the PIUs. They range from complete API⁹¹¹ to “[a]ll forms of payment information.”⁹¹² And regarding the numbers of affected passengers, it must be recalled that Article 2 expands its application to intra-EU flights. Member states may apply the PNR scheme to all flights or, according to its number 3, only to “selected intra-EU flights [they consider] necessary in order to pursue the objectives of this Directive.”⁹¹³ By October 2020, 24 member states had notified the Commission that they wished to apply it to intra-EU flights.⁹¹⁴ The 2020 review indicates that only one member state has decided not to collect PNR receipts from intra-EU flights.⁹¹⁵

According to Eurostat, in 2019, there were 518 952 085 passengers carried on extra-EU flights.⁹¹⁶ Together with the number of intra-EU international flights,⁹¹⁷ 873 690 283 passengers

⁹⁰⁷ Stoeva, 2014: 579.

⁹⁰⁸ Joined cases C-293/12 and C-594/12, paragraph 20.

⁹⁰⁹ Opinion 1/15, paragraph 36.

⁹¹⁰ *Idem*, paragraph 122.

⁹¹¹ Heading 18 of Annex I of Directive (EU) 2016/681.

⁹¹² Heading 6 of Annex I of Directive (EU) 2016/681.

⁹¹³ Article 2(3) of Directive (EU) 2016/681.

⁹¹⁴ European Commission, 2021. These member states are Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Finland, France, Germany, Greece, Italy, Latvia, Lithuania, Luxembourg, Hungary, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Spain, Sweden, and the United Kingdom.

⁹¹⁵ Report (COM(2020) 305 final, 24.7.2020), 10.

⁹¹⁶ Eurostat, 2021.

⁹¹⁷ According to Article 3, item (3), of Directive (EU) 2016/681, this does not include exclusively national flights, i.e., flights that do not cross member states’ borders.

were carried that year.⁹¹⁸ An “unlimited number”⁹¹⁹ is a hyperbolic figure of speech, in PNR as in relation to the data retention Directive. Nonetheless, it serves to raise awareness of the number of people that can be affected by data retention policies and the difficulties involved in targeting only a selected few with such wide data systems.

Moreover, PNR data are to be retained in the databases of the PIUs “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.”⁹²⁰ Even amidst criminal investigations, this is a long period for which to retain personal data. In fact, Article 6 of Directive 2006/24/EC held that member states could retain information between six and 24 months. If the Constitutional Court of Austria found this to be a long time, 60 months can surely be categorized as such.

The interference provoked by PNR is, nonetheless, different. Article 5 of Directive 2006/24/EC enshrined categories of information to be held, specifically communications and internet access metadata. The Court claimed that these data, taken as a whole, could lead to rather detailed findings on the privacy of data subjects, like their daily routines, activities, social interactions, and general whereabouts.⁹²¹ This is not the case here. Tzanou rightly highlights that it is not possible to draw such conclusions from PNR.⁹²²

With PNR, it is possible to make only a few inferences on residence, movement, and some of the activities carried out by passengers. The intensity of the intrusion is markedly different. Conversely, PNR allows for the mapping of the travel patterns of air passengers and the drawing of conclusions on other aspects of their lives, from dietary habits to work affiliation. There is an interference with the privacy of data subjects, even if it is not based on a systematic transmission of location and communications metadata. Although the interference is different, PNR data provide “the means...of establishing a profile of the individuals concerned.”⁹²³ This is a key aspect of the system to achieve its purposes, much as in other counter-terrorism legislation, such as Directives 2002/58/EC or 2006/24/EC. In relation to all of these, regardless of whether the information collected is content data or metadata, the profiling of data subjects and the sensitivity of the material collected clearly give rise to an interference with the fundamental rights of the individuals affected.

⁹¹⁸ Eurostat, 2021.

⁹¹⁹ Joined cases C-293/12 and C-594/12, paragraph 20.

⁹²⁰ Article 12(1) of Directive (EU) 2016/681.

⁹²¹ Joined cases C-293/12 and C-594/12, paragraph 27.

⁹²² Tzanou, 2017: 162.

⁹²³ Joined cases C-203/15 and C-698/15, paragraph 99.

The “possibility of establishing a profile of the persons concerned on the basis of...data”⁹²⁴ is one of the arguments the CJEU now uses to conclude that interferences with the rights foreseen in Articles 7 and 8 CFREU are particularly serious. This will be studied in section 2.3 below. For now, it suffices to say that the question is not if there is an interference, but how far it extends into the personal sphere of consumers. Retaining data, and permitting public authorities to access them, definitely affects privacy.

The data retention Directive regulated the “obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them.”⁹²⁵ The judges considered that retaining and using data as was provided for in that Directive “directly and specifically”⁹²⁶ fell within the scope of Article 8 CFREU since they are processing operations performed upon personal data. In fact, retaining data does not only affect privacy. It also affects the protection of that data. This was reinforced by the fact that the data retention Directive provided for local law enforcement agencies to have access to personal data for the “purpose of the investigation, detection and prosecution of serious crime.”⁹²⁷

Article 1(1)(a) of the PNR Directive says it regulates the “transfer by air carriers of passenger name record...data of passengers of extra-EU flights.”⁹²⁸ And item (b) adds that it provides for “the processing of the data referred to in point (a), including its collection, use and retention by Member States and its exchange between Member States.”⁹²⁹ It is easy to spot the similarities.

Both Directives regulate processing operations of personal data, beginning with their retention. As this is done by entities other than the data subjects themselves, this means that the processed data do not belong to the processors, or controllers. This is sufficient to invoke the data protection guarantees enshrined in Article 8 CFREU. Despite addressing different economic activities, both texts provide for systems that are built upon the processing of big personal data. Therefore, the argument that Directive 2006/24/EC could interfere with data protection can be replicated for Directive (EU) 2016/681.

⁹²⁴ Case C-623/17, paragraph 71.

⁹²⁵ Article 1(1) of Directive 2006/24/EC.

⁹²⁶ Joined cases C-293/12 and C-594/12, paragraph 29.

⁹²⁷ Article 1(1) of Directive 2006/24/EC.

⁹²⁸ Article 1(1)(a) of Directive (EU) 2016/681.

⁹²⁹ Article 1(1)(b) of Directive (EU) 2016/681.

2.2 When does the interference take place?

In *Digital Rights Ireland*, the Court found that interferences with privacy happened at two moments: when providers collected data and when national authorities accessed them. It did not answer this question regarding the right to data protection. Yet, in *Opinion 1/15*, it can be seen that interferences with data protection happen when data are processed.⁹³⁰

In PNR, service providers, in this case, carriers, collect and use data⁹³¹ which are then accessed, retained, processed, and exchanged by authorities of the member states. These are, first, the PIUs⁹³² and, then, other law enforcement agencies, either from the member states⁹³³ or third countries.⁹³⁴ Europol is also entitled to request PNR data.⁹³⁵

The scheme for data processing and transfer found in the data retention Directive, as well as in the Agreement with Canada, is replicated in the intra-EU system. There is, however, a relevant difference. In PNR, authorities not only access data collected and processed by private actors, but they process them too. While in Directive 2006/24/EC, national authorities only accessed what was supplied by services providers, in PNR they play a more active role, subjecting the data to further processing, over and above that already carried out by air carriers.

This is clear from the verbs used in its Article 1(1). It reads that the Directive provides for the “transfer by air carriers of passenger name record (PNR) data”⁹³⁶ and for “the processing of the data...by Member States.”⁹³⁷ The focus is upon the member states’ competent authorities. Air companies should only be concerned with transferring data as they receive them from booking and reservation procedures. How they process such data and how they handle and use them beyond this obligation seems irrelevant for the purposes of the Directive, provided data are not altered or abridged.

In *Opinion 1/15*, the CJEU identified a set of provisions that gave rise to concrete interferences with privacy and data protection. They were Articles 3, 4, 6, 8, 12, 15, 16, 18, and 19 of the Agreement, which ranged from the use of data to their sharing with police and judicial authorities, as well as retention and disclosure in and outside Canada. Access to data by parties other than their respective data subjects may give rise to an interference with fundamental

⁹³⁰ *Opinion 1/15*, paragraphs 125 and 126.

⁹³¹ Articles 1(1)(a) and 8 of Directive (EU) 2016/681.

⁹³² Articles 4(2)(a) and 6(1) of Directive (EU) 2016/681.

⁹³³ Articles 1(1)(b), 4(2)(b), 6(6), 7, and 9 of Directive (EU) 2016/681.

⁹³⁴ Article 11 of Directive (EU) 2016/681.

⁹³⁵ Articles 4(2)(b) and 10 of Directive (EU) 2016/681.

⁹³⁶ Article 1(1)(a) of Directive (EU) 2016/681.

⁹³⁷ Article 1(1)(b) of Directive (EU) 2016/681.

rights. If this idea was already gaining traction in joined cases C-293/12 and C-594/12, it was consolidated in Opinion 1/15.

2.3 Is the interference serious?

AG Cruz Villalón argued that the interference provoked by the data retention Directive was very serious.⁹³⁸ Although only metadata were to be collected, the system allowed for the retention of big troves of information in massive archives.⁹³⁹ This could generate a feeling of constant surveillance in the time during which data were retained.⁹⁴⁰ And this was a threat, as Brendan Lord said, to individual autonomy.⁹⁴¹

The CJEU agreed with the AG in classifying the interference as extensive and serious. It also commented that, as data subjects were unaware of their personal information being gathered and processed, this was sure to leave people with the impression that their lives were being continually monitored.⁹⁴²

A similar system was created by the PNR Agreement, which foresaw that the data of all passengers were to be systematically transferred to Canada.⁹⁴³ The Court found this to seriously interfere with their right to data protection. This was aggravated by the fact that data were to be processed by machines on a constant basis, even before airplanes landed in Canada.⁹⁴⁴

The PNR Directive allows for the collection, retention, transfer, and processing of big data in huge databases. These operations are to be performed on a continuous and systematic basis, making the interferences with the rights of air passengers serious, together with the fact it allows for the processing of content data, not only metadata. And passengers are likewise not informed when operations take place, which can trigger that chilling perception of constant surveillance.

A few scholars have, nonetheless, questioned this argument.

2.3.1 Systemic indifference

Some authors claim that modern societies and most individuals are becoming acquainted with, and perhaps indifferent to, the retention and processing of data – even personal data –, as this

⁹³⁸ Opinion of AG Cruz Villalón, paragraph 70.

⁹³⁹ *Idem*, paragraphs 71 and 72.

⁹⁴⁰ *Idem*, paragraph 72.

⁹⁴¹ Lord, 2019: 268. See also De Hert & Papakonstantinou, 2015: 161.

⁹⁴² Joined cases C-293/12 and C-594/12, paragraph 37.

⁹⁴³ Opinion 1/15, paragraph 127.

⁹⁴⁴ *Idem*, paragraph 131.

is done systematically, on a daily basis, and for a wide range of purposes. For Andrew Roberts, while many people believe that their:

[I]nterests [are] harmed when the state requires those who provide us with communications services to retain information about the way in which we use those services...[o]thers may well take a more sanguine view, doubting whether it can properly be said that the mere retention of such information amounts to any interference with privacy at all, or if it does, that it ought to be considered a relatively trivial interference. It might be said that mere retention of communications data will have no obvious effect on the lives of the great majority of those in respect of whom data [are] retained. Views on what ought to be required by way of justification for the retention of data are likely to vary in a way that corresponds roughly with divergence of views on the value of privacy and gravity of the interference that individuals suffer where communications data are retained.⁹⁴⁵

The Court has taken an important position in this discussion. It has joined the ranks of those claiming that retaining personal data causes a serious violation of privacy rights, which should therefore always be based on a certain level of reasonable suspicion. And even in such cases, personal data should not be retained in block but in a targeted manner. The judges have firmly opposed the logic of “the ‘needle in a haystack argument’ [where] mass data retention [is used to] ensure that a few vital pieces of information are available to the state for the purposes of detecting and investigating serious crime.”⁹⁴⁶

Despite this portrayal of the case law, the discussion is far from over and the intra-EU PNR may add fuel to the fire. Most passengers do not know what PNR stands for, let alone how the data are used. Even if they knew, many would likely be indifferent. So, the question is whether this serves to undermine the seriousness of the interference.

It probably does not. Nor does it dispel the unease some passengers would feel if they knew about the full journey of their data. A PNR system has the capacity to make a person experience “an immediate and involuntary shift in perspective [once she] becomes aware that others have information about her that she would rather they did not have.”⁹⁴⁷

In its referral to the CJEU, the Constitutional Court of Austria stressed that the people most likely to be affected were those whose actions do not justify their information being collected.⁹⁴⁸ The same could be said about PNR, making it important to explore the argument of Roberts,

⁹⁴⁵ Roberts, 2015: 535.

⁹⁴⁶ Ibidem. The author draws on the work of Nick Taylor regarding global surveillance in a comparison between the United Kingdom and the US (Taylor, 2014).

⁹⁴⁷ Idem: 543. See also Rössler, 2005: 116.

⁹⁴⁸ Joined cases C-293/12 and C-594/12, paragraph 20.

that many data subjects do not know that their information are collected, and act without fully knowing the consequences of their actions. Plus, most individuals who realize what may happen to their data “are likely to perceive the risk of suffering any material harm as a consequence of retention to be so remote that this knowledge is unlikely to affect their decision-making.”⁹⁴⁹

Yet, is this entirely true, or fair? In the PNR Directive as much as in the data retention Directive, consumers are required to provide big troves of personal data simply because they want access to services that are part and parcel of the fabric of modern life. And it is ludicrous to portray life nowadays without telecommunications, or air transportation. Therefore, the issue is not so much that consumers will carry on regardless of the consequences but that they simply cannot withdraw from using such services. Consumers, in fact, do not have a real choice between rights and services. The choice element is merely a formality and not a substantive exercise of volition and decision-making.

For that author, collecting such data results in a “loss of privacy [where] others...acquir[e] dominating power [over] the individual who has suffered the loss.”⁹⁵⁰ These laws are insidious, since they make access to essential services dependent on passively condoning serious interferences with fundamental rights.

To say that the interference provoked by pervasive data retention systems may not influence the actions of affected individuals because most of them are unaware of such systems, or seem not to care, is a misconception. They simply need to access the services provided, despite their new additional cost when measured in terms of fundamental rights. By contrast with the viewpoint of this scholar, a serious interference is present. The encroachment upon fundamental rights happens regardless of individuals being unaware of these systems and regardless of feeling adverse offline effects. And it happens even if numerous consumers cannot, or are not willing, to protect their rights. This apparent lack of awareness is less an indication of the users’ indifference, than of the iniquity of the law. As Tzanou rightly put it:

The data subject [gives] his consent for the processing of his data from the airline company in order to purchase a ticket, but no consent [is] given for the transfer of the data to intelligence and law enforcement authorities and data subjects cannot object to giving their PNR data if they wish to travel...Indeed, there is no issue of consent, but rather a ‘take it or leave it’ deal. As one airline CEO astutely put it: ‘You want to travel on the airline system? You give up your privacy. You don’t want to give up your privacy? Don’t fly.’⁹⁵¹

⁹⁴⁹ Roberts, 2015: 543 and 544.

⁹⁵⁰ *Idem*: 544.

⁹⁵¹ Tzanou, 2017: 167. In the last sentence, the author was quoting from Attanasio, 2002: 19.

2.3.2 A recent red line

Notwithstanding the previous debate and the questions it raises, the Court has recently established a standard that will further help to decide whether a data retention system can be considered to interfere seriously with the privacy and other fundamental rights of data subjects. While the Court's standard is in its infancy and is conservative in orientation, it seems to mark the beginning of drawing a red line on the matter.

As mentioned above, the fact that data could be used for establishing profiles, and that sensitive material could be collected, have been sufficient criteria for the judges to claim that certain data systems “allow [for] very precise conclusions to be drawn concerning the private lives of the persons whose data ha[ve] been retained.”⁹⁵² In light of this, they concluded, in the recent cases *Tele2*, *Privacy International*, and *La Quadrature du Net*, that there had been serious interferences with the rights to privacy and data protection.⁹⁵³

It is true that the Court did not discuss the idea of profiling in joined cases C-293/12 and C-594/12, or Opinion 1/15. Yet, this should not prevent us from transposing this red line to the assessment of the intra-EU PNR case. The analysis in this final part of chapter 3 draws inspiration from all the case law of the CJEU to help in assessing PNR.

While the case law is developing and starting to have an impact on the automated handling of personal data, it remains incomplete and the present remarks will inevitably reflect this. The intra-EU PNR does allow for the setting of profiles and for the collection of sensitive data without sufficient protection. The discussion here will be limited to profiling, with the question of the sufficiency of protection being parked till a later stage in the analysis.

Profiling has been assessed in some depth in chapter 3.1, with the authors surveyed claiming that it is a process of classifying and treating people according to pre-determined criteria.⁹⁵⁴ The Court is yet to table its own definition of the concept and this may well turn out to be a next important step in the jurisprudence. In any event, while the PNR Directive avoids using the term, this does not prevent profiling from taking place during the processing of data. In fact, to profile seems inherent in the system, which aims to sort through people to identify those “who require further examination by the competent authorities.”⁹⁵⁵ The literature is broadly consensual in considering that profiling occurs in PNR, with only the MEP Timothy Kirkhope

⁹⁵² Joined cases C-511/18, C-512/18 and C-520/18, paragraph 117.

⁹⁵³ See joined cases C-203/15 and C-698/15, paragraph 99, and C-623/17, paragraph 71.

⁹⁵⁴ Enerstvedt, 2017: 285.

⁹⁵⁵ Article 6(2)(a) of Directive (EU) 2016/681.

having publicly argued that it does not happen. Indeed, the sort of profiling that takes place in the PNR system is one of its most preoccupying features since passengers may be classified in a way that human operators do not entirely understand,⁹⁵⁶ but on the basis of which they must take relevant decisions, including those relating to the possible detention of individuals.

It is not necessary to comment on the nature of profiling taking place in PNR. It has been demonstrated that data collected under Directive (EU) 2016/681 provide “the means of establishing a profile of the individuals concerned”⁹⁵⁷ and it will be demonstrated later that that data, which are content data, can contain sensitive elements whose collection and processing are prohibited, in light of the CFREU. Therefore, it has been established at this stage that, under the criteria set out in the recent jurisprudence of the CJEU and also considering the arguments previously tabled in this section, the PNR Directive seriously interferes with the fundamental rights of air passengers.

Now that the interference occurring in PNR has been outlined, there are four questions that need answering. The first is whether such interference has been provided for by law. It then needs to be seen if it encroaches upon the essence, or core, of the affected rights, and if this piece of legislation pursues objectives of general interest recognized by the Union. The last question concerns the proportionality of PNR. The adequacy of the norms of the Directive for achieving its purposes will be discussed, along with whether they interfere with privacy and data protection only to the extent that it is strictly necessary to do so. The forthcoming sections answer these four questions.

3. Provided for by law

The first question is easy to answer. This criterion is readily satisfied as a Directive is a source of legal norms in EU law.⁹⁵⁸ In the words of Cruz Villalón, any limitations to privacy stemming from a Directive are objectively provided for by law, under Article 52(1) CFREU.⁹⁵⁹

⁹⁵⁶ See, for instance, the processing steps referred to in Articles 6(2)(c), 6(3)(b), or 6(4) of Directive (EU) 2016/681.

⁹⁵⁷ Joined cases C-511/18, C-512/18 and C-520/18, paragraph 117. Similar expressions can be found in joined cases C-203/15 and C-698/15, paragraph 99, and C-623/17, paragraph 71.

⁹⁵⁸ Article 288 TFEU.

⁹⁵⁹ Opinion of AG Cruz Villalón, paragraph 108.

4. The essence of the rights

The second question concerns the respect for the essence of the rights affected by the intra-EU PNR. Just like in chapter 3.2, it will be argued that this type of data retention system may interfere with the core of privacy and data protection rights. If the following arguments were accepted by the CJEU, this would suffice for it to declare the Directive invalid. Yet, even where the essence of a right is respected, secondary law can still be declared invalid for failing to fill the remaining criteria. The legal analysis will answer the other questions and undertake a full proportionality test, just as the Court did in *Digital Rights Ireland* and *Opinion 1/15*.

4.1 To privacy

Unlike the previous criterion, it is unclear whether the essence of the right to privacy is kept in PNR. For the Court, the core of privacy was respected in the data retention Directive, as it did not allow law enforcement to access content data.⁹⁶⁰

Still, it claimed that the remittance and precision of data in Directive 2006/24/EC could lead to rather accurate findings on the personal life of EU consumers.⁹⁶¹ PNR does not involve that level of monitoring, but big data are collected at a continuous rate. Moreover, it allows for the processing of all forms of payment,⁹⁶² general remarks that may include dietary or religious preferences,⁹⁶³ and API.⁹⁶⁴

In *Opinion 1/15*, the CJEU affirmed that the essence of privacy was likewise respected. It argued that, while PNR receipts may, in certain circumstances, disclose detailed material on the lives of passengers, the scope of such data has to do only with a part of those lives, namely air travels.⁹⁶⁵ This applies to the PNR Directive. The only meaningful difference between the lists of collected data lies in the fact that the Directive foresees the collection of “[a]ll forms of payment information, including billing address,”⁹⁶⁶ while the Agreement excluded “transaction details linked to a credit card or account and not connected to the travel transaction.”⁹⁶⁷ The

⁹⁶⁰ Joined cases C-293/12 and C-594/12, paragraph 39.

⁹⁶¹ *Idem*, paragraph 27.

⁹⁶² Heading 6 of Annex I of Directive (EU) 2016/681.

⁹⁶³ Heading 12 of Annex I of Directive (EU) 2016/681.

⁹⁶⁴ Heading 18 of Annex I of Directive (EU) 2016/681.

⁹⁶⁵ *Opinion 1/15*, paragraph 150.

⁹⁶⁶ Heading 6 of Annex I of Directive (EU) 2016/681.

⁹⁶⁷ Heading 8 of the Annex of Agreement (12657/5/13 REV 5, 23.6.2014).

Directive appears to have a wider scope, but this does not mean that PNR data collected under it are not related only to a part of the lives of passengers.

However, the Court's position is not consensual. Kuner, for example, says that he has not managed to find:

[A] common thread...that would identify the essence of the rights to private life and data protection. One can argue that the essence of a fundamental right cannot be described in abstract terms and can only be determined based on the circumstances of a particular case...However, the need for clarity and predictability makes it important to develop a normative framework for determining the essence of [a] right...which the Court has thus far not done for the rights protected by Articles 7 and 8 of the Charter.⁹⁶⁸

As in previous holdings, the CJEU seems to have only scratched the surface of the problems concerning the essence of privacy. It is not possible to ascertain where it lies or what its content is. By saying, in *Digital Rights Ireland*, that the data retention Directive did not infringe the essence of privacy because only metadata were collected⁹⁶⁹ and, in *Opinion 1/15*, that its core was kept intact because the data collected only concerned air transportation,⁹⁷⁰ it is not evident where the CJEU finds the essence of privacy. It appears that, either its position is outdated in relation to present technologies,⁹⁷¹ or that the essence of privacy is extremely narrow.

It is difficult to use the case law as a tool to assess EU secondary law. That is the practical effect Kuner seems to have in mind when speaking of the “need for clarity and predictability”⁹⁷² in the jurisprudence. The Court should be clear so that interpreters can find the tools to evaluate similar norms. Those tools should be predictable so that the results of subsequent interpretations can lead to clear outcomes.

This problem begins with the CJEU devoting only one paragraph to the matter in both joined cases *C-293/12* and *C-594/12* and *Opinion 1/15*. This raises more questions than it provides answers — questions with real consequences, not least since the essence of fundamental rights must not be limited. If the Court does not clarify where the essence of privacy lies, then its opinion that the data retention Directive and the Agreement do not encroach upon such an essence cannot even be understood in full, let alone contested.

⁹⁶⁸ Kuner, 2018: 876.

⁹⁶⁹ Joined cases *C-293/12* and *C-594/12*, paragraph 39.

⁹⁷⁰ *Opinion 1/15*, paragraph 150.

⁹⁷¹ Ojanen, 2014: 537.

⁹⁷² Kuner, 2018: 876.

Ojanen thinks that the mere transferring of metadata in large quantities suffices to violate the essence of privacy. Following his reasoning, if the most robust techniques for gathering and processing metadata may be viewed as interfering with the sacrosanct essence of the right to privacy,⁹⁷³ applying these to content data certainly constitutes a violation of its essence. From this point of view, the PNR Directive disrupts the core of privacy. The CJEU would probably disagree, but maybe incorrectly.

The remark that PNR data only concern a part of the lives of data subjects also deserves some scrutiny. First, the Directive applies to all international flights.⁹⁷⁴ It is not only data of passengers traveling to Canada that are stored. It is the data of any passenger who flies to any destination outside his or her departing country. Not only are there more individuals whose privacy is violated, but, from an individual perspective, the potential for interference has increased. It is not only when flying to Canada that data are retained but whenever individuals fly anywhere outside the Union or, possibly, even just outside the member states.

Second, it is not self-evident that the scope of PNR data regards only a limited part of their lives.⁹⁷⁵ In fact, it is hard to pinpoint relevant personal content data that are not included in PNR receipts. The logic of the system is, precisely, to leave nothing out so as to allow the “identification of persons who were unsuspected of involvement in terrorist offences or serious crime prior to such an assessment.”⁹⁷⁶

Kuner believes that the CJEU will eventually lay down a theoretical roadmap to help outline the essence of privacy and data protection.⁹⁷⁷ It might be that such a time will come when the Directive is challenged in court. So far, evidence of respect for the essence of privacy is very scant. If this system permits law enforcement to know the content of air passengers’ bookings automatically, systematically, and *en masse*, allowing for unprecedented identification, where is the untouched core of privacy?

4.2 To data protection

In *Digital Rights Ireland*, the judges found that the essence of data protection was respected by the data retention Directive, since its Article 7 imposed upon private actors key principles to

⁹⁷³ Ojanen, 2014: 537.

⁹⁷⁴ Articles 1(1)(a) and 2 of Directive (EU) 2016/681.

⁹⁷⁵ Opinion 1/15, paragraph 150.

⁹⁷⁶ Recital (7) of Directive (EU) 2016/681.

⁹⁷⁷ Kuner, 2018: 876.

protect data and make them secure.⁹⁷⁸ They reached a similar conclusion about the Agreement, claiming its Article 3 limited the processing undertaken by the CBSA and Article 9 laid down rules to maintain the security and integrity of data.⁹⁷⁹

While the essence of privacy seems to be violated in the intra-EU PNR, the case might be different regarding data protection. Its essence is affected if minimum conditions for processing information foreseen in Article 8 CFREU are not respected. This means, if secondary law does not: i) allow data subjects to protect their personal data;⁹⁸⁰ ii) ensure data are “processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law;”⁹⁸¹ iii) guarantee “the right of access...and the right to have [data] rectified;”⁹⁸² and iv) provide for “control by an independent authority.”⁹⁸³

The Directive appears to meet these requirements. Firstly, its Article 13 foresees a series of individual data rights. It states that “every passenger shall have the same right to protection of their personal data, rights of access, rectification, erasure and restriction and rights to compensation and judicial redress.”⁹⁸⁴

The legislation also includes provisions that, read together, keep the processing of data fair, i.e., free from bias, errors, or injustice. Again, Article 13 obliges member states to provide for the implementation of rules on “confidentiality of processing and data security [applicable] to all processing of personal data.”⁹⁸⁵ It also adds that the system is “without prejudice to the applicability of Directive 95/46/EC...to the processing of personal data by air carriers, in particular their obligations to take appropriate technical and organisational measures to protect the security and confidentiality of personal data.”⁹⁸⁶ Moreover, it prohibits the processing of data based on unlawful criteria, that is, elements that could lead to negative discrimination, according to Article 21 CFREU.⁹⁸⁷

On the other hand, Article 6(5) instructs member states to “ensure that any positive match resulting from the automated processing of PNR data...is individually reviewed by non-

⁹⁷⁸ Joined cases C-293/12 and C-594/12, paragraph 40. See also Article 7 of Directive 2006/24/EC.

⁹⁷⁹ Opinion 1/15, paragraph 150.

⁹⁸⁰ Article 8(1) CFREU.

⁹⁸¹ Article 8(2) CFREU.

⁹⁸² *Idem*.

⁹⁸³ Article 8(3) CFREU.

⁹⁸⁴ Article 13(1) of Directive (EU) 2016/681.

⁹⁸⁵ Article 13(2) of Directive (EU) 2016/681.

⁹⁸⁶ Article 13(3) of Directive (EU) 2016/681. The provisions applicable are now from the GDPR.

⁹⁸⁷ This is repeated in Articles 6(4) and 7(6) of Directive (EU) 2016/681.

automated means.”⁹⁸⁸ The same is supposed to happen before data are transmitted “for further examination to the competent authorities.”⁹⁸⁹ Article 12(5) also reads that the:

[R]esult of [data] processing...shall be kept by the PIU only as long as necessary to inform the competent authorities...of a positive match. Where the result of automated processing has...proven to be negative, it may, however, be stored so as to avoid future ‘false’ positive matches for as long as the underlying data are not deleted.⁹⁹⁰

Another relevant norm is Article 5, which orders PIUs to “appoint a data protection officer responsible for monitoring the processing of PNR data and implementing relevant safeguards.”⁹⁹¹ This is accompanied by Article 6(7), which instructs member states to “ensure that the data protection officer has access to all data processed by the PIU. If the data protection officer considers that processing of any data has not been lawful, [it] may refer the matter to the national supervisory authority.”⁹⁹²

The Directive also establishes that data should be processed only for “specified purposes.”⁹⁹³ This is reiterated throughout the text, starting with Article 1(2). It reads that “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.”⁹⁹⁴ PIUs requesting data from other member states can process⁹⁹⁵ data “only for [specified] purposes,”⁹⁹⁶ just like other national competent authorities.⁹⁹⁷ And transfers of data to third countries and among them⁹⁹⁸ are limited to the “purposes of this Directive.”⁹⁹⁹ These are only some examples. The text foresees that data can only be processed for specified purposes in many provisions.

The basis for the collection of data is not explicit consent.¹⁰⁰⁰ The CJEU examined this in Opinion 1/15, arguing that the processing of PNR data must find another legitimate basis. This basis seems to overlap with the purposes of the Directive. The legitimacy of the system is

⁹⁸⁸ Article 6(5) of Directive (EU) 2016/681.

⁹⁸⁹ Article 6(6) of Directive (EU) 2016/681.

⁹⁹⁰ Article 12(5) of Directive (EU) 2016/681.

⁹⁹¹ Article 5(1) of Directive (EU) 2016/681.

⁹⁹² Article 6(7) of Directive (EU) 2016/681.

⁹⁹³ Article 8(2) CFREU.

⁹⁹⁴ Article 1(2) of Directive (EU) 2016/681.

⁹⁹⁵ Article 9(2) of Directive (EU) 2016/681.

⁹⁹⁶ Articles 6(2) and (3)(a) of Directive (EU) 2016/681.

⁹⁹⁷ Article 7(1) of Directive (EU) 2016/681.

⁹⁹⁸ Article 11(1)(c) of Directive (EU) 2016/681.

⁹⁹⁹ Article 11(1)(b) of Directive (EU) 2016/681.

¹⁰⁰⁰ Article 8(2) CFREU.

justified by the fight against terrorism and serious crime, cited throughout the text¹⁰⁰¹ and in the recitals.¹⁰⁰² It is likewise grounded upon the need to “enhance internal security, to gather evidence and, where relevant,^[L]^[SEP] to find associates of criminals and unravel criminal networks.”¹⁰⁰³

The Directive likewise provides for control by an independent authority. Such control is undertaken internally and externally, and by more than one entity. Internally, PIUs must appoint a DPO “for monitoring the processing of PNR data and implementing relevant safeguards.”¹⁰⁰⁴ And Article 15 regulates external control, instructing member states to guarantee that there is a national supervisory authority “responsible for advising on and monitoring the application within its territory of the provisions adopted by the Member States.”¹⁰⁰⁵ They should conduct their supervision “with a view to protecting fundamental rights in relation to the processing of personal data.”¹⁰⁰⁶ That provision refers to Article 25 of Framework Decision 2008/977/JHA for details. The key aspect to highlight is that this norm specifies that supervisory authorities “shall act with complete independence in exercising the functions entrusted to them.”¹⁰⁰⁷

These references lay out a set of minimum conditions which ensures that the essence of data protection is guaranteed in the Directive. This does not mean such provisions are adequate to protect the information and data subjects, or that they are proportionate. These remarks only refer to the core of the fundamental right to data protection.

The failure to meet one of these cumulative criteria is enough for the Court to declare that EU secondary law violates the CFREU.¹⁰⁰⁸ This legal analysis could end here in light of the

¹⁰⁰¹ Articles 1(2), 4(1), 6(2) and (3), 7(1), (2), and (4), 8(5), 9(2) and (4), 10(2), 11(2)(a), and 12(4) of Directive (EU) 2016/681.

¹⁰⁰² Recitals (6), (7), (10), (15), (22), (23), (25), (35), and (38) of Directive (EU) 2016/681.

¹⁰⁰³ Recital (6) of Directive (EU) 2016/681.

¹⁰⁰⁴ Article 5(1) of Directive (EU) 2016/681.

¹⁰⁰⁵ Article 15(1) of Directive (EU) 2016/681.

¹⁰⁰⁶ Article 15(2) of Directive (EU) 2016/681.

¹⁰⁰⁷ Article 25 of Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350, 30.12.2008). This Decision has been repealed by Directive (EU) 2016/680. Still, the idea of independence was fully maintained in this Directive, keeping the purpose and logic of Article 15(1) of Directive (EU) 2016/681 when it says that “Article 25 of Framework Decision 2008/977/JHA shall apply.” In fact, Directive (EU) 2016/680 emphasizes this aspect, the independence of supervisory authorities. Its Chapter VI is titled “[i]ndependent supervisory authorities,” with section 1 discussing their “[i]ndependent status.” Article 41, which regulates these authorities, says that “independent public authorities [shall] be responsible for monitoring the application of this Directive, in order to protect the fundamental rights and freedoms of natural persons in relation to processing.” And Article 42 is dedicated to their status of independence. Its number 1 reads that “[e]ach Member State shall provide for each supervisory authority to act with complete independence in performing its tasks and exercising its powers in accordance with this Directive.” There are other provisions that could be worth mentioning but these suffice to demonstrate that the independence of the authorities exercising external control over the processing of data is explicitly guaranteed in the PNR Directive, read together with Directive (EU) 2016/680.

¹⁰⁰⁸ Ojanen, 2014: 533.

encroachment upon the essence of the right to privacy. This would be a precarious approach, nevertheless, as the Court might disagree, especially considering its case law. As things stand, it is thus preferable to answer all of the questions mentioned above, and apply a proportionality test. The next step is to ascertain whether the Directive pursues objectives of general interest recognized by the Union.

5. Objectives of general interest recognized by the EU

This is the last criterion that needs to be discussed before undertaking the proportionality test. The purpose of Directive 2006/24/EC was to guarantee the availability of personal data to fight crime and maintain public security.¹⁰⁰⁹ The CJEU claimed that providing for the retention of data to allow law enforcement to use them satisfied an objective of general interest.¹⁰¹⁰

Article 1(2) of the PNR Directive reads that “PNR data collected...may be processed only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime.”¹⁰¹¹ It partially mimics Article 1(1) of Directive 2006/24/EC, which stated that the information “generated or processed [was to be] available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.”¹⁰¹²

There are some differences between the Directives. The first difference that is relevant from a legal point of view concerns the insertion of the particle ‘only.’ This actually increases the legal certainty of the PNR system, by preventing the use of any data beyond what is explicitly permitted in the text. It limits the margin of discretion of member states, Europol, and third countries, as well as of all actors accessing and processing PNR.

The second difference regards the use of personal data not only to investigate, detect, and prosecute crimes but also to prevent them. This widens the purposes for which data may be processed, and it may not be the best development from the perspective of fundamental rights. Still, it is aligned with the rationale defended by the Court, as preventing crime through the use of data serves to fight it and maintain security.

A final remark is about the addition of the fight against terrorism as an objective underpinning the PNR Directive. This similarly does not weaken the claim that PNR pursues a

¹⁰⁰⁹ Joined cases C-293/12 and C-594/12, paragraph 41.

¹⁰¹⁰ *Idem*, paragraph 44.

¹⁰¹¹ Article 1(2) of Directive (EU) 2016/681.

¹⁰¹² Article 1(1) of Directive 2006/24/EC.

general security interest recognized by the EU. The nature and shape of terrorist acts are substantively akin to that of serious crimes. Article 3, paragraph (8), of Directive (EU) 2016/681 defines terrorist acts as those “offences under national law referred to in Articles 1 to 4 of Framework Decision 2002/475/JHA.”¹⁰¹³ According to those norms, and those which have replaced them, terrorist actions are those that “may seriously damage a country or an international organisation,”¹⁰¹⁴ such as attacks upon a person’s life or physical integrity, kidnapping, hostage-taking, or acts that cause extensive destruction to endanger human life or result in major economic loss.¹⁰¹⁵ These are all examples of serious crimes. They are only classified as terrorism because of the motives behind their execution, as well as their context.

There is another argument supporting the claim that the fight against terrorism can be deemed as an objective of general interest recognized by the EU. And it can be distilled directly from the case law of the Court.

It was established in chapter 2 that the CJEU considers that terrorist activities can affect national security and that national security is a societal interest of greater relevance for the member states and the Union than public security, or fighting serious crime.¹⁰¹⁶ In the cases *Tele2* and *La Quadrature du Net*, the judges inverted the expression normally used to acknowledge that certain pieces of secondary law serve objectives of general interest. Instead of saying something like “the material objective of that directive is...to contribute to the fight against serious crime and thus, ultimately, to public security,”¹⁰¹⁷ they said that “[g]iven the seriousness of the interference in the fundamental rights concerned represented by national legislation...only the objective of fighting serious crime is capable of justifying such a[n interference].”¹⁰¹⁸ In *La Quadrature du Net*, the Court added the goals of preventing “serious threats to public security”¹⁰¹⁹ and the “safeguarding of national security.”¹⁰²⁰

¹⁰¹³ Framework Decision (2002/475/JHA) is no longer in force as it has been repealed by Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017). All references to this Decision, like what happens with Framework Decision 2008/977/JHA, are therefore outdated, and should be read as referring to Directive (EU) 2017/541 instead.

¹⁰¹⁴ Articles 1(1) of Council Framework Decision (2002/475/JHA) and 1(1) of Directive (EU) 2017/541.

¹⁰¹⁵ References taken from Articles 1(1)(a) to (d) of Council Framework Decision (2002/475/JHA) and of Directive (EU) 2017/541.

¹⁰¹⁶ To recall, in cases *C-623/17*, paragraph 75, and *C-511/18*, *C-512/18* and *C-520/18*, paragraph 136, the judges wrote that the “importance of the objective of safeguarding national security, read in the light of Article 4(2) TEU...goes beyond...the objectives of combating crime in general, even serious crime, and of safeguarding public security.”

¹⁰¹⁷ Joined cases *C-293/12* and *C-594/12*, paragraph 41.

¹⁰¹⁸ Joined cases *C-203/15* and *C-698/15*, paragraphs 102 and 115. Similarly, see joined cases *C-511/18*, *C-512/18* and *C-520/18*, paragraph 156.

¹⁰¹⁹ Joined cases *C-511/18*, *C-512/18* and *C-520/18*, paragraph 140.

¹⁰²⁰ *Idem*, paragraph 156.

This means that the minimum threshold for the judges to accept that any given law is capable of justifying a serious interference with fundamental rights in the area of security is if it does so for the purposes of fighting serious crime, preventing threats to public security, or safeguarding national security. In the case *La Quadrature du Net*, they actually seem to present these purposes in specific order of importance when affirming that “the objectives of combating serious crime, preventing serious attacks on public security and, a fortiori, safeguarding national security are capable of justifying...the particularly serious interference entailed by the targeted retention of traffic and location data.”¹⁰²¹ Even if this last sentence were missing, it stands to reason that, if fighting serious crime and ensuring public security *lato sensu* are less important purposes than countering terrorism and guaranteeing national security, EU and member state legislation aiming at the latter purposes necessarily meet objectives of general interest recognized by the EU.

It is true that the Court has elsewhere considered that fighting terrorism is within the scope of the “fight against serious crime,”¹⁰²² or has placed these objectives side by side.¹⁰²³ This does not help at making matters clearer but it likewise does not endanger the inquiry pursued in this section of ascertaining whether the PNR Directive serves a general interest recognized by the Union. The minimum requirement is met either way.

It can hence be argued that the Directive pursues a general security interest. Curiously, however, and in line with the Court’s inclusion of counterterrorism in the fight against serious crime, PNR appears to serve to fight both “terrorist offences and serious crime.”¹⁰²⁴ The legislator weaved together what may now be considered, from a narrow perspective, two security objectives placed at different levels of importance: one related to national security and the other to public security. This does not encroach upon the argument made in this section as, again, the minimum threshold identified above is attained. Yet, it shows two things.

On the one hand, it shows the evolution and consolidation of the Court’s reasoning on justifications for large-scale surveillance;¹⁰²⁵ by distinguishing between levels of security and societal interests, tabling a minimum requirement for EU secondary law and local legislation to interfere with fundamental rights, and admitting that national security and counterterrorism

¹⁰²¹ Joined cases C-511/18, C-512/18 and C-520/18, paragraph 146.

¹⁰²² Joined cases C-203/15 and C-698/15, paragraph 103.

¹⁰²³ Joined cases C-511/18, C-512/18 and C-520/18, paragraph 122.

¹⁰²⁴ Article 1(2) of Directive (EU) 2016/681.

¹⁰²⁵ Such evolution and consolidation are clearly taking form due to the fact that the CJEU is reiterating and developing its case law on the difference between the objective of safeguarding national security and purposes like maintaining public security or fighting serious crime. See, in particular, cases C-623/17, paragraphs 74 and 75, and C-511/18, C-512/18 and C-520/18, paragraphs 135 and 136.

are fundamental values of such importance for the member states that the Union should not be entirely free to decide on such matters. On the other, it shows how confusing this whole security terminology is and why there is urgent need for some sort of agreed catalogue of matters that fall under the different types of security, just as the House of Lords argued back in 2008.¹⁰²⁶

The CJEU took a similar view in Opinion 1/15. It considered that the Agreement aimed at ensuring public security through fighting terrorism and serious international criminal offenses.¹⁰²⁷ This was and remains an “objective of general interest of the European Union that is capable of justifying even serious interferences with the fundamental rights enshrined in Articles 7 and 8 of the Charter.”¹⁰²⁸

Despite the nuances, there is an overarching security purpose common to Directive 2006/24/EC, the EU-Canada PNR Agreement, and Directive (EU) 2016/681. This is mirrored in the continuity of the rationale present in the case law. Moreover, security is explicitly mentioned in the opening provisions of the PNR Directive.¹⁰²⁹ If anything, it is conceivable that its final text has improved legal certainty and security, at least as regards PNR serving a general interest recognized at EU level.

6. The principle of proportionality

Recital (22) of the PNR Directive states that “the application of this Directive should ensure full respect for fundamental rights, for the right to privacy and for the principle of proportionality.”¹⁰³⁰ According to this logic, its transposition and enforcement should “meet the objectives of necessity and proportionality in order to achieve the general interests recognised by the Union...in the fight against terrorist offences and serious crime.”¹⁰³¹ In order to do so, the use of PNR should be “duly justified and the necessary safeguards [must be] put in place to ensure the lawfulness of any storage, analysis, transfer or use of PNR data.”¹⁰³²

It seems the legislator was trying to prove the overall proportionality of the Directive. Despite this attempt, this chapter argues that it is disproportionate. While it may be adequate to serve its goals, it goes beyond that which is strictly necessary to do so. The interference with

¹⁰²⁶ European Union Committee of the House of Lords, 2008, paragraph 6.241.

¹⁰²⁷ Opinion 1/15, paragraph 148.

¹⁰²⁸ *Idem*, paragraph 149.

¹⁰²⁹ Its recital (5), for instance, says that “[t]he objectives of this Directive are, inter alia, to ensure security,” and recital (11) adds that “[t]he processing of personal data should be proportionate to the specific security goals pursued by this Directive.”

¹⁰³⁰ Recital (22) of Directive (EU) 2016/681.

¹⁰³¹ *Idem*.

¹⁰³² *Idem*.

fundamental rights does not seem justified and the legislation should be reviewed to comply with Articles 7, 8, and 52 CFREU.

It is important to note that including this proportionality assessment does not undermine the criticisms set out above. The claim that the Directive violates the essence of privacy, for example, remains intact. Yet, if the CJEU were to consider otherwise, the next steps would be to discuss its adequacy and necessity, the two components of the principle of proportionality that the Court tends to explore when ruling on the validity of legislation in the AJSJ.

The discussion on the adequacy of PNR is relatively brief since the Directive appears to be adequate in terms of its capacity to contribute to its goals as it stands. Yet, the following sections are very complex. This legal analysis tries to take a considerable step forward in comparison to previous literature and even the argumentation of the CJEU in *Digital Rights Ireland* and *Opinion 1/15*. The claim that PNR is not limited to that which is strictly necessary is based on the quantity and quality of data that are collected and processed in the system, the length of and uncertainty surrounding the data retention period, and the problems concerning access rights by third parties. A final criticism, although beyond the structure of the proportionality test, arises from the lack of embedded individual notification procedures.

Each of these sections is divided into subsections which mainly correspond to the specific criteria that can be distilled from the case law, as well as the from the contributions of other sources analyzed above. The section on the data retention period, for instance, examines, *inter alia*, whether the Directive tables objective criteria justifying the retention of data, whether data and passengers are categorized according to their relevance for law enforcement purposes, and whether the system ensures that data are irreversibly eliminated by the end of the retention period. This unpacking of larger themes allows for a more careful assessment of those aspects which do not appear to be limited to that which is strictly necessary to achieve the Directive's goals. Beyond that, and as far as possible, this analysis also tries to emulate what the Court did in *Opinion 1/15*, by explaining what should have been done differently, and how norms could be redrafted, to make PNR comply with what the CJEU thinks are the acceptable standards for the retention and processing of big data.

6.1 Adequacy

The judges were rather vague in discussing the adequacy of Directive 2006/24/EC and of the PNR Agreement. They started by noting that the proportionality principle entails that EU

secondary legal acts must be adequate to achieve their purposes and should not go beyond that which is strictly necessary to do so.¹⁰³³

Retaining PNR data allows law enforcement agencies to have supplementary tools to better understand violent and complex crime. PNR can be a key instrument in fighting it, not because of the “growing importance of means of electronic communication”¹⁰³⁴ but due to the growing importance of air travel. The Court said as much in Opinion 1/15. Following a report from the Commission from 2010,¹⁰³⁵ it found that assessing data before the arrival of travelers to Canada was an appropriate way to improve security and border controls. This reasoning also applies to the PNR Directive, which tables a similar system to prevent, detect, investigate, and prosecute crime and terrorism.¹⁰³⁶

There is an additional aspect that merits discussion. Mrs. Tschohl and Seitlinger, as well as the Portuguese Government, submitted, in their written observations to joined cases C-293/12 and C-594/12, that there were many types of telecommunications which were not covered by the data retention Directive. For them, this rendered the Directive inadequate to attain its goals. The Court thought otherwise, claiming that, while this could reduce the capacity of the Directive to achieve its goals, it did not make it inadequate.¹⁰³⁷

The same holds true, *mutatis mutandis*, regarding the intra-EU PNR. It targets only air travel, leaving member states free to choose what they want to do about other means of transport. Yet, this does not render it inappropriate. On the contrary, a limited scope makes it less pervasive and potentially more respectful of fundamental rights.

6.2 Strict necessity

A large majority of scholars considers that the Directive is not limited to that which is strictly necessary to achieve its purposes. Yet, it should be noted that few suggest viable alternatives that could improve the system and ensure that it does not interfere with fundamental rights in an unacceptable way.

This section will go through the practical details of this piece of legislation, to explain the core reasons why PNR appears to interfere with the privacy and data protection of passengers in a manner that goes beyond that which is strictly necessary to achieve the purposes of public

¹⁰³³ Joined cases C-293/12 and C-594/12, paragraph 46.

¹⁰³⁴ *Idem*, paragraph 49.

¹⁰³⁵ Communication (COM(2010) 492 final, 21.9.2010), section 2.2.

¹⁰³⁶ Article 1(2) of Directive (EU) 2016/681.

¹⁰³⁷ Joined cases C-293/12 and C-594/12, paragraph 50.

security at which it aims. While this analysis does not question the need for a European PNR or the importance of such purposes, it considers that the means deployed to achieve these exceed what is necessary, just like in the data retention Directive and the Canada Agreement.

6.2.1 Quantity and quality of collected data

A. A matter of quantity

There are two key problems which the Court may (and ought to) identify in the Directive regarding the necessity of the quantity of data retained in the system. The first concerns the amount of collected data, as well as its effects upon data subjects. The second is the legal uncertainty stemming from how its Annex I is currently drafted.

A.1 The amount of collected data

The CJEU argued in *Digital Rights Ireland* that the retention of all telecommunications data from all data subjects interfered with the rights and freedoms of virtually every EU citizen.¹⁰³⁸ Moreover, Directive 2006/24/EC did not distinguish individuals based on their relevance for its purposes.¹⁰³⁹ It affected people whose behavior seemed to have no direct or indirect connection with serious criminal offenses.¹⁰⁴⁰ Such concerns can be transposed to the PNR Directive, as it provides for the retention of all booking data of all passengers of all extra EU-flights.¹⁰⁴¹

As the Court would clearly lay out in *Tele2*, member states may adopt data retention measures to fight and prevent serious crime but national provisions, and EU norms for that matter, must be limited to allowing only targeted retention. Adapting the case law to PNR, this means that collecting passengers' information for surveillance purposes must be limited "with respect to the categories of data to be retained...the persons concerned and the retention period adopted...to what is strictly necessary."¹⁰⁴²

A further step was taken in another recent case, *La Quadrature du Net*, when the judges stated that the retention of sensitive data must be the exception, not the rule, and established

¹⁰³⁸ Joined cases C-293/12 and C-594/12, paragraph 56.

¹⁰³⁹ *Idem*, paragraph 57.

¹⁰⁴⁰ *Idem*, paragraph 58.

¹⁰⁴¹ Article 1(1)(a) of Directive (EU) 2016/681. And, eventually, of all passengers of all intra-EU flights, according to its Article 2.

¹⁰⁴² Joined cases C-203/15 and C-698/15, paragraph 108.

limits on the scope and durability of retention periods.¹⁰⁴³ The Court likewise summarized the standards for finding data retention practices lawful, establishing that it is only allowed:

[T]he targeted retention of traffic and location data for the purposes of combating serious crime, preventing serious threats to public security and equally of safeguarding national security, provided that such retention is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.¹⁰⁴⁴

It is not certain, from the perspective of a doctoral thesis, whether this recent case law and its strict approach to validity, should be transposed, as such, to assess PNR. These cases evince a very strong position that would arguably suffice to justify the invalidity of the Directive because it explicitly does not abide by most of these parameters in a straightforward way.

It is true that many of the Court's criteria in these recent cases resonate with Opinion 1/15 and have already been used in this work to criticize the intra-EU system. This is because PNR is not based on the targeted retention of data, but on a systematic and continuous collection of all passenger records that ignores categories of data, the persons concerned, or a limited retention period. Plus, these records refer to content data, not metadata like in online and telecommunications data. However, as will also be discussed in the section on access by public authorities to PNR, the cases *Tele2*, *La Quadrature du Net*, and even *Digital Rights Ireland* are built upon a consolidated line of cases on the retention and processing of traffic and location data. It may be premature, at this moment, to apply these standards bluntly to the analysis of the PNR Directive, which has so far had very little attention in the case law of the CJEU.

This is not to reject the relevance of these criteria but simply to argue in favor of a careful approach which focuses on Opinion 1/15. Recent pronouncements from the Court do not leave the reader indifferent and they may well mark the beginning of the end for present and future large-scale surveillance operations that, *inter alia*, are not targeted, aim at all categories of data and all persons, regardless of their relevance for the purposes of those operations, and depend on the unceasing transfer of material. Yet, it is best, for now, to adopt a cautious reading of the jurisprudence on telecommunications data and to criticize PNR based on criteria that also stem from Opinion 1/15. Already, this provides sufficient ammunition to argue that the intra-EU PNR should be invalidated on various grounds.

¹⁰⁴³ Joined cases C-511/18, C-512/18 and C-520/18, paragraph 142.

¹⁰⁴⁴ *Idem*, paragraph 147.

PNR has the potential to affect the rights of most EU citizens. The system can affect large numbers of people who seem to have no connection with serious crime or terrorism. The Union legislator appears to have assumed this on recital (7), when stating that using PNR data allows for the “identification of persons who were unsuspected of involvement in terrorist offences or serious crime prior to such an assessment.”¹⁰⁴⁵

It is true that that same recital also specifies that the system should be “limited to what is necessary”¹⁰⁴⁶ by controlling the offenses that can be investigated. It further stresses that it must ensure that the “minimum...number of innocent people [is] wrongly identified.”¹⁰⁴⁷ Yet, it seems that, in practice, the legislator ignored the red line of the Court of limiting the “categories of data to be retained [and] the persons concerned.”¹⁰⁴⁸

PNR, in fact, depends on the automatic retention of millions of data entries of air passengers with no differentiation between them, not even one based on previous criminal records, or criminal suspicion. It makes blanket retention the rule, rather than the exception, since it relies on the belief that monitoring the movements of innumerable unsuspected passengers will help in fighting crime efficiently, effectively, and in a timely manner. From this perspective, recital (7) is little more than an aspiration.

Beyond that, the Annex I of the Directive requires the collection of up to 19 items of data from each passenger. Concerns arise as to whether many of them are truly necessary.¹⁰⁴⁹ This enters in direct conflict with the data minimization principle. It appears the Directive fails to observe the first limitation that should be present in data retention schemes.

As mentioned, this limitation requires that there is a link between the categories of collected data, the people surveilled, and a security risk.¹⁰⁵⁰ PNR serves to investigate the background and whereabouts of air passengers to fight terrorism and serious crime. Although the public whose data should be supplied is clearly identified – air passengers – the system operates regardless of a specific, or objective, link, even an “indirect one, with serious criminal offences,”¹⁰⁵¹ or with “a serious risk to public security or a risk to national security,”¹⁰⁵² that justifies the collection of data in such a broad scale. Adapting the Court’s “geographical criterion,”¹⁰⁵³ PNR is not even limited to flights from dangerous areas.

¹⁰⁴⁵ Recital (7) of Directive (EU) 2016/681.

¹⁰⁴⁶ *Idem*.

¹⁰⁴⁷ *Idem*.

¹⁰⁴⁸ Joined cases C-203/15 and C-698/15, paragraph 108.

¹⁰⁴⁹ Tzanou, 2017: 171.

¹⁰⁵⁰ Joined cases C-293/12 and C-594/12, paragraph 59.

¹⁰⁵¹ Joined cases C-203/15 and C-698/15, paragraph 111.

¹⁰⁵² Joined cases C-511/18, C-512/18 and C-520/18, paragraph 148.

¹⁰⁵³ *Ibidem*. See also paragraph 150.

Taking one more step in this line of thought may irrefutably show how PNR matured in a manner that takes it far from these jurisprudential concerns regarding the quantity and categories of collected traffic and location data. It may be uncertain, for the time being, whether the Court will take this step when assessing the Directive but the fact is that the judges added that “it must be made clear that the persons...targeted [are] persons who have been identified beforehand, in the course of the applicable national procedures and on the basis of objective evidence, as posing a threat to public or national security in the Member State concerned.”¹⁰⁵⁴

This standard will be studied in depth below regarding access to data by law enforcement agencies. It can, however, already be said that it is consistent with the traditional premises of criminal procedure law, whereby people and data can only be investigated if there is a reasoned suspicion of the commission, or preparation, of criminal offenses. Yet, if we transpose this to PNR, it becomes visible how this traditional logic is being bent in favor of access to large troves of information. If the connection between categories of passengers, the data collected from them, and threats to security does not exist in PNR, it stands to reason that the information sent to the PIUs is certainly not related only to people and data that have been identified earlier in the context of a criminal investigation giving rise to a reasonable suspicion.

With Directive (EU) 2016/681, law enforcement can access all categories of PNR data and air passengers regardless the existence of a reasonable suspicion, or a formal investigation subject to prior review. This is a serious danger to which Paul De Hert and Rocco Bellanova already alerted us to in 2011.¹⁰⁵⁵

Besides, many of the elements collected are excessive, or redundant. They are required for no particular investigatory reason.¹⁰⁵⁶ Law enforcement does not need so much data from an *ex ante* perspective. In addition, as it has been showed before, neither the data retention limitation nor the link to serious crimes¹⁰⁵⁷ are within the scope of the PNR Directive. As mentioned, PNR is not collected only from people who are likely to be involved in serious crime or whose data might visibly contribute to fighting it. Instead, all data items are collected from every person, with no distinction based on their relevance or utility to law enforcement.

¹⁰⁵⁴ Joined cases C-511/18, C-512/18 and C-520/18, paragraph 149.

¹⁰⁵⁵ De Hert & Bellanova, 2011: 495.

¹⁰⁵⁶ According to Report (COM(2020) 305 final, 24.7.2020), 11, the Commission is considering applying “additional measures, such as the mandatory collection of the passengers’ date of birth by air carriers [which] may be necessary to enhance data quality.” There are no explanations as to how such data may be “important to allow for an even more targeted and efficient data processing.” Yet, it is relevant to note that the Commission decided to study all “[d]ata quality improvements” before suggesting them to the member states, or tabling “amendments to the PNR Directive.”

¹⁰⁵⁷ Joined cases C-293/12 and C-594/12, paragraph 59.

The CJEU did not go into the details of how only potentially relevant PNR data could be retained, or how the information could be collected in a targeted manner. Perhaps, these limitations might undermine the purpose and added value of PNR.¹⁰⁵⁸ Yet, there are mechanisms to mitigate the interference with privacy and data protection which could balance the tension between trying to know what is unknown and the need to protect fundamental rights. Mechanisms such as limits on the data retention periods, or more targeted collection goals. In any case, as things stand, the Directive is not limited to what is strictly necessary to safeguard these rights, considering the amount and diversity of data that are collected by the system.

Therefore, if the Court has prohibited EU¹⁰⁵⁹ and national legislation from providing for the “general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication,”¹⁰⁶⁰ it may well be that EU and local laws providing for the general and indiscriminate retention by all “air carriers of [all] passenger name record (PNR) data of [all] passengers of [all] extra-EU flights”¹⁰⁶¹ and, possibly, all intra-EU flights¹⁰⁶² will be likewise prohibited.

A.2 Legal uncertainty

The second problem concerning the proportionality of the quantity of data retained under the PNR Directive has to do with the legal uncertainty inherent in how Annex I is worded. The issue derives from vague and open-ended headings. Curiously, this is a problem that was already present in the Agreement with Canada. The Court said, in Opinion 1/15, that it should have been very clear regarding the information that carriers were expected to send to Canada.¹⁰⁶³ This echoed Mengozzi’s words when writing that some of the data categories to be collected were overly open, making it impossible for individuals to know what information could actually be included in the PNR receipts.¹⁰⁶⁴

The legislator should have avoided drafting another system with similar problems to those identified by the CJEU. And this was a soft ball. It shows the lack of effort put into preparing

¹⁰⁵⁸ According to its recital (9), “[t]he use of PNR data together with API data has added value in assisting Member States in verifying the identity of an individual, thus reinforcing the law enforcement value of that result and minimising the risk of carrying out checks and investigations on innocent people.”

¹⁰⁵⁹ Joined cases C-293/12 and C-594/12, paragraphs 56 ff.

¹⁰⁶⁰ Joined cases C-203/15 and C-698/15, paragraph 112.

¹⁰⁶¹ Article 1(1)(a) of Directive (EU) 2016/681.

¹⁰⁶² Article 2 of Directive (EU) 2016/681.

¹⁰⁶³ Opinion 1/15, paragraph 155.

¹⁰⁶⁴ Opinion of AG Mengozzi, paragraph 217.

and reviewing the legislation, and reinforces the suspicion that fear and haste guided the hand of the European legislator.

Headings 5, 7, and 17 of the Annex of the EU-Canada PNR Agreement were items deemed insufficiently specific.¹⁰⁶⁵ While the grammatical components that excessively opened headings 5 and 7 were eliminated in the corresponding entries in Annex I of Directive (EU) 2016/681,¹⁰⁶⁶ this did not happen in the case of heading 17, whose content was transposed to heading 12 of Annex I. They both allow for the collection of “general remarks.”¹⁰⁶⁷

There is, however, a difference between the entries. Heading 17 read that PNR receipts could contain “[g]eneral remarks including Other Supplementary Information (OSI), Special Service Information (SSI) and Special Service Request (SSR) information.”¹⁰⁶⁸ Whereas, heading 12 says that they may include:

General remarks (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).¹⁰⁶⁹

This difference is irrelevant as both refer to general remarks. Heading 12 can be criticized in much the same way as heading 17 was. It also appears to be a sort of “free text heading,”¹⁰⁷⁰ which sets no concrete limitations on the data that could be collected under it, thus falling short in terms of the degree of transparency and accuracy. While the drafters may have been thinking about different types of data, both entries allow for PNR receipts to include remarks aimed at making air services more personalized. However, these remarks may go well beyond what is strictly necessary, containing data that can serve discriminatory aims, or sensitive information, such as that regarding food or religious preferences, or even health conditions.

Therefore, Article 6(1), *in fine*, which states that “[w]here the PNR data transferred by air carriers include data other than those listed in Annex I, the PIU shall delete such data

¹⁰⁶⁵ Opinion 1/15, paragraph 156.

¹⁰⁶⁶ Heading 5 of the Annex of Agreement (12657/5/13 REV 5, 23.6.2014) used the expression “etc.” regarding the frequent flyer and benefit information that could be collected, whereas heading 8 of Annex I of Directive (EU) 2016/681 only mentions “[f]requent flyer information.” Likewise, heading 7 of the Annex of Agreement (12657/5/13 REV 5, 23.6.2014) referred to “[a]ll available contact information,” while heading 5 of Annex I of Directive (EU) 2016/681 speaks only of “[a]ddress and contact information,” detailing in brackets that this means “telephone number [and] e-mail address.”

¹⁰⁶⁷ Heading 17 of the Annex of Agreement (12657/5/13 REV 5, 23.6.2014) and heading 12 of Annex I of Directive (EU) 2016/681.

¹⁰⁶⁸ Heading 17 of the Annex of Agreement (12657/5/13 REV 5, 23.6.2014).

¹⁰⁶⁹ Heading 12 of Annex I of Directive (EU) 2016/681.

¹⁰⁷⁰ Opinion 1/15, paragraph 160.

immediately and permanently upon receipt,”¹⁰⁷¹ may be of little practical effect. Brendan Lord is mistaken in considering that this provision can render “this list exhaustive.”¹⁰⁷²

B. A matter of quality

If heading 17 of the Annex of the Agreement allowed for different kinds of data to be included in PNR receipts, this meant sensitive data could end up there. In Mengozzi’s view, this could be as varied as health, ethnic, or even religious data on air passengers.¹⁰⁷³

Such information can be relevant for air staff to satisfy the needs of passengers in more efficient ways, thus providing better and more customized services. Yet, they should not be used for security purposes. Javier Argomaniz argues that the problem is precisely that this use is possible in the Directive, as it was in the Agreement.¹⁰⁷⁴ Prohibited data can be collected and processed under the general remarks foreseen in heading 12.

The Court was clear in saying that any decision by means of which sensitive data could be relevant, despite the concrete behavior of passengers, would violate their privacy and the protection of their personal data, as well as amounting to negative discrimination. It added that sensitive information could only be sent to law enforcement if there was a specific public security reason.¹⁰⁷⁵ This was not the case in the Agreement, whose norms on data processing were, therefore, in violation of Articles 7, 8, and 21 CFREU.¹⁰⁷⁶

This is also not the case in the Directive, as it opens the door for the transmission of sensitive data to law enforcement in much the same way. Still, there is an important guarantee. Its Article 13(4) says that:

Member States shall prohibit the processing of PNR data revealing a person’s race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation. In the event that PNR data revealing such information are received by the PIU, they shall be deleted immediately.¹⁰⁷⁷

¹⁰⁷¹ Article 6(1) of Directive (EU) 2016/681.

¹⁰⁷² Lord, 2019: 265.

¹⁰⁷³ Opinion of AG Mengozzi, paragraph 221.

¹⁰⁷⁴ Argomaniz, 2009: 129 and 130.

¹⁰⁷⁵ Opinion 1/15, paragraph 165.

¹⁰⁷⁶ *Idem*, paragraph 167.

¹⁰⁷⁷ Article 13(4) of Directive (EU) 2016/681. This safeguard is also present in Articles 6(4) and 7(6). Article 6(4) says that the “assessment of passengers prior to their scheduled arrival in or departure from the Member State...shall be carried out in a non-discriminatory manner...The criteria shall in no circumstances be based on a person’s race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.” And Article 7(6) reads that “[t]he competent authorities shall not take any decision that produces an adverse legal effect on a person or significantly affects a person only by reason of the automated

Unlike the Agreement, the Directive seems to foresee that the processing of sensitive data is prohibited. This caveat was present in the 2011 proposal, as mentioned by the Dutch Senate.¹⁰⁷⁸ This could prevent negative discrimination against passengers. Adapting the words of AG Mengozzi, there is less risk of the PNR Directive “stigmatising a large number of individuals who are not suspected of any offence which the use of such sensitive data entails.”¹⁰⁷⁹

Nevertheless, sensitive data can still be used. Though Article 13(4) foresees trade union membership, health, and sexual life as prohibited criteria, there are elements present in Article 21 CFREU that have been left out. Sex, color, social origin, genetic features, language, membership of a national minority, property, birth, disability, or age are not mentioned in the Directive, despite being criteria upon which discrimination “shall be prohibited.”¹⁰⁸⁰

This insufficiency can also be traced back to the 2011 draft Directive. In fact, the Dutch Senate asked the legislator why nationality was not listed as a sensitive criterion, considering that the CFREU forbids discriminatory practices on such a basis.¹⁰⁸¹ Saulnier-Cassia is right in claiming that Article 13(4) has a more limited scope than Article 21 CFREU, which can render the prohibition on the processing of sensitive data, and the obligation for PIUs to delete them,¹⁰⁸² not entirely effective.¹⁰⁸³ This is an important criticism. The argument of Bogdan Bîrzu, that the scope of the Directive suffices to prevent negative discrimination because it expressly bans the use of sensitive data,¹⁰⁸⁴ is not compelling as a result. As it is currently drafted, it allows for sensitive data to be used by the PIUs, and there is a risk that they will also be available for other law enforcement units through heading 12 of Annex I.

The Directive is not limited to what is strictly necessary to respect the rights to privacy and data protection when it comes to both the quantity and quality of collected data. And this seems to derive from gross negligence on the part of the legislator. As far as quality is concerned, it could easily have been ensured that either a clause on general remarks was not included in the legislation, or that all elements whose processing is prohibited in the CFREU were expressly excluded from the system. Annex I could contain a specific heading for data on unaccompanied minors, without necessitating the introduction of the concept of general remarks.

processing of PNR data. Such decisions shall not be taken on the basis of a person’s race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.” The criteria used in these three provisions are the same, which gives coherence to the legal text but also reinforces the criticisms regarding their insufficiency under the CFREU.

¹⁰⁷⁸ Letter from René van der Linden, 1.

¹⁰⁷⁹ Opinion of AG Mengozzi, paragraph 222.

¹⁰⁸⁰ Article 21(1) CFREU.

¹⁰⁸¹ Letter from René van der Linden, 1.

¹⁰⁸² Articles 6(1) and 13(4) of Directive (EU) 2016/681.

¹⁰⁸³ Saulnier-Cassia, 2017: 217.

¹⁰⁸⁴ Bîrzu, 2016: 196.

The following issue is heatedly debated. While the CJEU put forward certain criteria that data retention systems should meet, in order to guarantee that only necessary data are kept and processed by competent authorities, it did not give an opinion on how long they may retain data. The following sections will, therefore, demonstrate that PNR does not meet those basic criteria, and will present arguments that should persuade the Court to rethink its approach to the time limits governing the retention of personal data.

6.2.2 Data retention period

Article 6 of Directive 2006/24/EC gave a margin of discretion to member states regarding the data retention period. They should “ensure that the categories of data [were] retained for periods of not less than six months and not more than two years from the date of the communication.”¹⁰⁸⁵

Cruz Villalón considered that storing personal data online should be seen as an exceptional operation.¹⁰⁸⁶ In his view, retention schemes must not be common practice and retaining data should always be limited to that which is really necessary. In the case of the data retention Directive, he sustained that data should be retained for no more than one year¹⁰⁸⁷ and only particular conditions¹⁰⁸⁸ could justify longer periods.

The Court followed a different path. First, it pointed to the lack of objective standards for limiting the time span to that which was necessary.¹⁰⁸⁹ The problem was that national legislators did not have clear and objective parameters defined by EU secondary law upon which to determine concrete periods for retaining the information.

Second, it argued that setting a retention period not adapted to the different categories of data, or the status of passengers from a criminal law perspective, also goes beyond that which is strictly necessary. The CJEU considered that each element of collected data must be retained depending on its future utility to achieve the purposes of the legislation, and on the criminal conduct of the affected individuals.¹⁰⁹⁰ Despite the fact that Directive 2006/24/EC allowed member states to create different data retention periods under those criteria, the judges thought

¹⁰⁸⁵ Article 6 of Directive 2006/24/EC.

¹⁰⁸⁶ Opinion of AG Cruz Villalón, paragraph 144.

¹⁰⁸⁷ *Idem*, paragraph 149.

¹⁰⁸⁸ *Idem*, paragraph 151.

¹⁰⁸⁹ Joined cases C-293/12 and C-594/12, paragraph 64.

¹⁰⁹⁰ *Idem*, paragraph 63.

the Directive ought to define such periods *ex ante*. Because it failed to do so, it did not manage to provide concise norms on the scope of the interference with privacy and data protection.¹⁰⁹¹

The judges added that the data retention Directive did not ensure that the data collected were permanently deleted upon the expiry of the retention period.¹⁰⁹² Four requirements can thus be derived from these comments, which can be used to verify the validity of data retention periods from the perspective of the proportionality principle. First, whenever the Union leaves the definition of concrete data retention periods to the discretion of member states, there must be clear and objective criteria defined by EU law that constrain such discretion to ensure that they are limited to that which is strictly necessary. Secondly, retention periods must be adapted to the different categories of data, or the nature of the data subjects, having regard to the purposes of the legislation. Additionally, systems must provide for the irreversible destruction of the information when the retention periods expire. And the final criterion is that these retention periods must be reasonably limited.

The first three are distilled from the case law. The final argument draws inspiration from the literature review, institutional discussions, and the opinions of AGs. It will be more extensively elaborated, precisely because it is not rooted directly in the case law.

A. Objective criteria

The PNR Directive appears to meet the first requirement. Article 12 does not set a range of possible retention periods in the same manner as Article 6 of the data retention Directive. It fixes a period of five years, in contrast to the provision that data should be stored for no “less than six months and [no] more than two years.”¹⁰⁹³ There is therefore no need for objective criteria to narrow the length of any concrete retention period decided by the member states.

However, the EU legislator did not explain why it chose five years, or why this period is strictly necessary for meeting the objectives pursued by the Directive, as the CJEU required.¹⁰⁹⁴ This is a topic that needs some unpacking.

What criteria could the judges have in mind to ensure that the legislator complies with the requirement of strict necessity? And how should these criteria be translated into legal provisions? These questions should be answered by the Court to help guide future legislation.

¹⁰⁹¹ Joined cases C-293/12 and C-594/12, paragraph 65.

¹⁰⁹² *Idem*, paragraph 67, *in fine*.

¹⁰⁹³ Article 6 of Directive 2006/24/EC.

¹⁰⁹⁴ Joined cases C-293/12 and C-594/12, paragraph 64.

As it stands, it might be difficult for legislators to elaborate legislation on PNR, or other data-based systems, in a lawful way. And it becomes likewise hard to judge such systems' compliance with the requirement of strict necessity.

After these initial questions, the case law prompts consideration of whether the EU legislator should make explicit the criteria it uses to determine a single period for data retention. When member states have no margin of discretion, ought it not to be possible for them to know the criteria justifying the choice for a particular period? This is a matter of transparency, as well as of legal certainty and security. Yet, if this is so, the PNR Directive fails to meet this requirement. It contains no criteria justifying a retention period of 60 months, nor does it explain how such a period can be understood as limited in accordance with the principle of strict necessity.

Article 12(2) determines that data must be depersonalized six months after having been collected. However, there are problems with the depersonalization mechanisms included in the Directive and there are exceptions allowing for longer retention periods. These mechanisms will be addressed when discussing the final criterion. In any event, masking out data does not invalidate the claim that the personal files of air passengers are retained for a long period of time, which is not based upon objective criteria laid down in EU law. From this angle, the intra-EU PNR does not justify, in objective terms, the necessity of the interference with the rights to privacy and to the protection of data.

B. Categories of data and relevance of passengers

Tailoring retention periods according to different categories of information and the relevance of data subjects from the point of view of the system's objectives can place a heavy burden on legislatures. Again, the Court did not develop its argument extensively, thus leaving some questions unanswered.

Authors like Giulia Tiberi and Francesca Di Matteo point to the fact that the Directive does not link the categories of information to specific retention periods.¹⁰⁹⁵ A similar concern had already been expressed by member states when they were asked whether the 2011 proposal respected fundamental rights. The Austrian National Council feared that five years was too long, considering that data were stored irrespective of any concrete individual suspicion.¹⁰⁹⁶ This was supported by the Dutch Senate, which said that retaining data from people who are

¹⁰⁹⁵ Tiberi, 2016: 592, and Di Matteo, 2017: 232.

¹⁰⁹⁶ Mitteilung vom 5. April 2011, 2.

not criminal offenders may lead to unlawful profiling.¹⁰⁹⁷ The German Federal Council further added that doing so without a just cause, i.e., an attributable conduct with a certain dangerous nature, is a particularly serious limitation of the rights to informational self-determination and to private life.¹⁰⁹⁸

This subject was raised by Mengozzi in his assessment of the Agreement. Not having different time periods for different categories of data made him wonder:

[W]hether, after several years, there [was] justification for retaining certain categories of data...In particular, [he] wonder[ed] whether...information only about the actual carrier prove[d]...to...having genuine added value by comparison with the other data which [were] also retained and which may be unmasked, with the aim of combating terrorism and serious transnational crime.¹⁰⁹⁹

The concerns expressed here may hint at a possible solution. A simple way to enforce this obligation is to have data retained for different periods depending on the relevance of passengers from the point of view of criminal law. The CJEU was willing to accept the long data retention period enshrined in the EU-Canada Agreement, the same five years now foreseen in the PNR Directive, provided that only data of passengers under suspicion were retained after their departure from Canada. In contrast, storing data from every passenger despite his or her connection with terrorism and serious crime¹¹⁰⁰ was neither lawful, nor limited to that which is strictly necessary.¹¹⁰¹

It stands to reason that, for the EU PNR to fulfil this requirement, there could be rules for processing and retaining data belonging to “persons who require further examination by the competent authorities,”¹¹⁰² and other provisions applicable to passengers cleared in PNR assessments and security checks. The latter should not have their full data retained for five years. A more balanced approach could be to keep their information for 24 hours, 30 days, or six months. One possibility would be to keep all data for 24 hours and only crucial elements which may serve criminal investigations for 30 days, six months, or even five years, depending on the complexity of the specific investigations.

¹⁰⁹⁷ Letter from René van der Linden, 1.

¹⁰⁹⁸ Beschlussdes (6007/11), paragraph 7.

¹⁰⁹⁹ Opinion of AG Mengozzi, paragraph 284.

¹¹⁰⁰ Opinion 1/15, paragraph 205.

¹¹⁰¹ Idem, paragraphs 206 and 211.

¹¹⁰² Article 6(2)(a) of Directive (EU) 2016/681.

These suggestions are not arbitrary. 24 hours is what happens with API.¹¹⁰³ 30 days was the suggestion of the EDPS in 2011. It claimed that “[n]o data should be kept beyond 30 days in an identifiable form, except in cases warranting further investigation.”¹¹⁰⁴ And six months is the time mentioned in the Directive before depersonalization takes place.¹¹⁰⁵ Although half a year can also be considered a long period from the viewpoint of air passengers with no criminal record, it would be a solution that is more sensitive to privacy and data protection, and to the stated ambitions of the legislation, to seek out the “persons who were unsuspected of involvement in terrorist offences or serious crime prior to such an assessment and who should be subject to further examination.”¹¹⁰⁶ The invisible dots and connections that PNR can bring to light viz. other existing security mechanisms could still be identified with more limited and tailored data retention periods, and it would still be within the timeframe considered reasonable by AG Cruz Villalón, who maintained that data should be retained for no more than a year.¹¹⁰⁷

PNR is based on the premise that big data related to the journeys of passengers should be kept for a long time so that law enforcement can access them to connect invisible dots and find suspicious patterns of movement in criminal investigations. This was what the Commission and the Council argued before the Court, clinging to the complexity of such investigations to sustain the necessity of collecting and retaining all categories of data belonging to all passengers for such a long period. They argued that the estimated lifetime of transnational complex criminal networks and the length of related investigations justified long retention periods.¹¹⁰⁸

As mentioned above, the Court agreed up to a point. It did not find that retaining the data of all passengers was limited to that which is strictly necessary, because this applied also to passengers who had not been identified as giving rise to a risk of terrorism or serious transnational crime.¹¹⁰⁹ Only when there is concrete proof of such a risk is it acceptable to retain data after their return flight.¹¹¹⁰ This is a strong stand for fundamental rights but one which, in a way, directly contravenes the logic of PNR.

The judges similarly criticized the data retention Directive since it did not provide only for the collection of the data elements that could prove useful for its law enforcement purposes.¹¹¹¹ Directive (EU) 2016/681 similarly does not distinguish between categories of data to be

¹¹⁰³ Article 6(1), 3rd and 4th paragraphs, of Council Directive 2004/82/EC.

¹¹⁰⁴ Opinion of the EDPS (OJ C 181, 22.6.2011), paragraph 57.

¹¹⁰⁵ Article 12(2) of Directive (EU) 2016/681.

¹¹⁰⁶ Recital (7) of Directive (EU) 2016/681.

¹¹⁰⁷ Opinion of AG Cruz Villalón, paragraph 149.

¹¹⁰⁸ Opinion 1/15, paragraph 204.

¹¹⁰⁹ *Idem*, paragraphs 204 to 206.

¹¹¹⁰ *Idem*, paragraph 207.

¹¹¹¹ Joined cases C-293/12 and C-594/12, paragraph 63.

retained. In practice, all the booking data of all air passengers must be collected and retained in the PIUs for the full duration of five years. The system allows for the retention of the personal content of PNR receipts for a long period with no strong reason or justification, thereby circumventing the protective logic of Article 8 CFREU.

It is notable that the legislator managed to commit the same mistake regarding similar legislation. Failing to read the case law of the CJEU can seriously undermine an entire legal and policy agenda, enfeebling legal certainty and security, as well as throwing in the bin the time, resources, and effort put into the preparation of the legislation.

C. Irreversible destruction of data

The final requirement concerning the data retention period that can be explicitly distilled from the case law has to do with the elimination of retained data. This issue is going to be addressed in this section.

The Court asserted that the data retention Directive failed to guarantee that data were completely eliminated by the expiry of the retention period and, thus, did not ensure the necessary high level of protection and safety.¹¹¹² Article 12 of Directive (EU) 2016/681 regulates this matter, with Article 12(4) saying that “Member States shall ensure that the PNR data are deleted permanently upon expiry”¹¹¹³ of the retention period. Yet, it immediately adds that this “obligation shall be without prejudice to cases where specific PNR data have been transferred to a competent authority and are used in the context of specific cases for the purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious crime.”¹¹¹⁴

This means that data that have been copied, processed, or saved, partially or in full, by authorities other than the PIUs, can be retained in a manner that is not subject to control by the Directive. So, even if the PIUs must delete them, other law enforcement authorities are free from this obligation. They are not even required to demonstrate that such data are needed in the context of ongoing investigations. The excerpt “in the context of specific cases”¹¹¹⁵ allows for the scope of undetermined situations to be broadly defined.

This exception undermines the system’s capacity to guarantee the complete elimination of data that were collected under its scope and for its purposes. The chain of control of EU law

¹¹¹² Joined cases C-293/12 and C-594/12, paragraph 67.

¹¹¹³ Article 12(4) of Directive (EU) 2016/681.

¹¹¹⁴ *Idem*.

¹¹¹⁵ *Idem*.

over the personal information of air passengers is interrupted, should the PIUs transfer data to other authorities. And such transfers are part and parcel of the normal processing of PNR;¹¹¹⁶ they are not exceptional situations in which only certain PNR receipts could end up being occasionally scattered in different databases.

The Directive does, indeed, “provide for the retention of PNR data in the PIUs for a period of time not exceeding five years, after which the data should be deleted.”¹¹¹⁷ But given the way in which it is currently drafted, this is not sufficiently tight to comply with the data retention principle. This principle is associated with other principles, such as purpose limitation, proportionality, and minimization. It requires that “data should not be kept unnecessarily...to reduce the risk of the data becoming inaccurate, outdated or irrelevant [and] to enhance data security, reducing chances of data misuse.”¹¹¹⁸

This type of openness in a data system is particularly worrying, in Olga Enerstvedt’s view, when the personal information of suspect and innocent data subjects is gathered in the same way. As seen above, PNR foresees for the retention of data regardless the relevance of air passengers from a criminal law perspective. It circumvents the need to set strict data collection policies, and to keep assessing such procedures on a regular basis, to guarantee respect for individual privacy and data protection.¹¹¹⁹

The disregard for an exhaustive and complete elimination of the information¹¹²⁰ by means of that exception, means that the interference with fundamental rights extends beyond the strictly necessary for the purposes of the Directive. Actually, it would already be doubtful whether member states could control the disposal of data by all the entities that can request PNR, even if the Directive did not foresee for this exception. Its express inclusion confirms the gap between the published PNR and the case law of the CJEU.

The Directive fails to meet the requirements set forth by the judges in *Digital Rights Ireland* and *Opinion 1/15* regarding the retention period. This should not only be a matter of concern to passengers, but also serve to militate in favor of the invalidity of this piece of legislation. There is, however, another aspect worth debating regarding data retention periods, which has not been explored in depth by the Court.

Scholars have often claimed that PNR receipts are held for an excessively long time, be it in the 2011 proposal, the external agreements, or the 2016 Directive. The Court has ignored these

¹¹¹⁶ Articles 6(2)(a) and (b) of Directive (EU) 2016/281.

¹¹¹⁷ Recital (37) of Directive (EU) 2016/681.

¹¹¹⁸ Enerstvedt, 2017: 195.

¹¹¹⁹ *Idem*: 196.

¹¹²⁰ Joined cases C-293/12 and C-594/12, paragraph 67.

claims so far. The following sections take such claims on board, to expose the issues arising from a long retention period, to shed light on how long data can, in practice, be kept for in the databases of law enforcement authorities, and to suggest ways of mitigating the problems of an excessively long data retention period.

This chapter does not claim that the CJEU should have a one-size-fits-all approach to data retention schemes. What it suggests, instead, is that personal data should not be retained for very long, let alone indefinite, periods of time. The EU legislator should strive to tailor these periods and to ensure that they are reasonably limited. This would be more possible to achieve if the judges were to play a more active role in defining the limits for data retention periods.

D. Reasonable limitation

The Court only referred to this issue in Opinion 1/15. It first mentioned that the period in the EU-Canada Agreement had been prolonged in relation to the 2006 Agreement by a year and a half. The judges found this to be still acceptable under the objectives of the legislation, agreeing with the Council and the Commission that the complexity of serious crime and criminal investigations sufficed to sustain a retention period of five years.¹¹²¹

The judges were willing to accept long periods provided there was a link between the retained data and the purposes of the legislation. It appears they did not feel empowered to ascertain whether five years is a short or a long term, sufficient or not, to allow law enforcement to conduct criminal investigations. That is a matter for the legislator to decide, together with experts. As the explanations of the Council and the Commission did not seem absurd or excessive, they found no problems with the retention period.

This position ignored what the AG had written in his observations. He said that the concrete motivations of the Commission and Canada for setting such a lengthy data retention period were not clear.¹¹²² Mengozzi confessed to having concerns regarding the strict necessity of five years.¹¹²³ He is not alone in this opinion.

Georgios Nouskalis thinks that it amounts to a disproportionate breach of privacy rights.¹¹²⁴ The EDPS has continually opposed such long data retention periods¹¹²⁵ and it would be later joined by Giulia Tiberi, who emphasizes the fact that the Directive provides for a retention

¹¹²¹ Opinion 1/15, paragraphs 205 and 209.

¹¹²² Opinion of AG Mengozzi, paragraph 279.

¹¹²³ *Idem*, paragraph 285.

¹¹²⁴ Nouskalis, 2011: 476.

¹¹²⁵ Opinion of the EDPS (OJ C 181, 22.6.2011), paragraph 43.

period that is longer than any other included in previous internal policies or legislation, even the invalidated Directive 2006/24/EC.¹¹²⁶ The question, for now, is whether the Court is still willing to accept such long data retention periods, even if there is a connection between the retained data and the objectives pursued.

The problem in Opinion 1/15, as identified by Arianna Vidaschi, is that the CJEU did not expressly discuss the duration of the retention period. It limited itself to brief remarks on this issue, seeing that it is a complex and sensitive matter to regulate.¹¹²⁷ The judges simply accepted the specified time period, without questioning or problematizing it, let alone clarifying their views. They used the complexity of criminal investigations to excuse themselves from further exploring this matter.

Only in the recent case *La Quadrature du Net*, has the Court made a comment that marks the possible beginning of jurisprudence establishing the need to shorten the time during which personal data are retained for investigatory purposes. It mentioned that “competent authorities [can only] order providers of electronic communications services to retain traffic and location data...for a limited period of time.”¹¹²⁸ And it added that the “instruction for the preventive retention of data... must...be limited in time to what is strictly necessary.”¹¹²⁹ Although it can be “renewed, the duration of each instruction cannot exceed a foreseeable period of time.”¹¹³⁰ This strengthens the argument of this section, stressing the need to have reasonable time limits when allowing for the retention of data by, or under the instruction of, law enforcement.

There are two issues, however, that make this case law insufficient in terms of building a robust argument against the length of PNR’s data retention period. On the one hand, it only refers to the retention of data by private actors, not public bodies. The problems associated with private air carriers retaining PNR for a long time will be discussed later in the chapter and raise many concerns. Yet, the main issue arising in relation to the PNR system actually involves public agencies retaining and processing data themselves for a very long time. On the other hand, the Court only said that the retention of information should be limited to that which is strictly necessary. But how long is this? What are the criteria, or framing standards, to consider that a certain retention period is longer, or not, than justified? By not elaborating on the length of prospective periods of time, it is difficult, if not impossible, to use this case law, as it stands, to find parameters to criticize PNR by reference to concrete timespans. It cannot even be argued

¹¹²⁶ Tiberi, 2016: 592.

¹¹²⁷ Vidaschi, 2018: 425.

¹¹²⁸ Joined cases C-511/18, C-512/18 and C-520/18, paragraph 137.

¹¹²⁹ *Idem*, paragraph 138.

¹¹³⁰ *Ibidem*.

with certainty that the Court is no longer willing to accept long data retention periods because it is still not clear what constitutes a long, or short, period of time for the CJEU.

Given the limitations inherent in this recent case law, the legal constraints established by Opinion 1/15 therefore remain highly relevant. Nonetheless, the case *La Quadrature du Net* does open up useful perspectives which reinforce the conclusions drawn on the basis of Opinion 1/15. Considering this, it remains crucial to discuss, in more depth, the need to have short, reasonable, and foreseeable data retention periods.

This work has no sufficient authority to go against rulings of the CJEU. It can only question the precedent that remains here due to the lack of parameters to assess the length of retention periods. It is unclear why a period of five years does not exceed that which is strictly necessary to fight crime, even if only data of people with criminal records were collected. Would the Court have accepted it now, after issuing its decision in the *La Quadrature du Net* case? This also leads to the question of how far the Commission and the Council could have extended the retention period, while still persuading the Court that it was necessary, based on concepts such as the complexity of criminal investigations, or the longevity of criminal networks. The fact that no clear criterion to reasonably limit the data retention period is defined in the case law, beyond foreseeability, leaves member states and EU institutions with few tools to evaluate what is necessary, or proportionate.

The CJEU could pay attention to the literature and the viewpoints of the auxiliary bodies to consider shorter periods. It merely censured what was easy to go after in the Agreement: retaining data from passengers with no direct, or indirect, connections to serious crime or terrorism at the time of collection. This was visibly unnecessary and disproportionate, as much from the perspective of privacy as from purpose specification, or the right to data protection. That is why it did not engage in extensive argumentation when declaring unlawful the “continued storage of the PNR data of all air passengers.”¹¹³¹ Yet, the judges should be more sophisticated in their reasoning.

In any event, and even accepting that the Court might admit the five-year retention period included in the Directive, the fact remains that the legislator ratified a very long period for retaining personal information, with no objective criteria showing why it is strictly necessary to attain the purposes of the system. Two other issues can be discussed in relation to this. The first concerns the depersonalization mechanisms enshrined in the Directive. It might be argued that they compensate for the lack of a short data retention period. Yet, this argument can be

¹¹³¹ Opinion 1/15, paragraphs 204 and 205.

challenged, as those mechanisms are not drafted in a satisfactory manner. The second problem concerns the potential renewal of PNR receipts, which causes three chilling effects. These chilling effects are associated with the fear that can build up among air passengers and EU consumers more broadly, that PNR, and eventually other data retention systems, might end up, *de facto*, allowing countless law enforcement agencies, in and outside the Union, to retain their personal data for an indefinite period of time. This is due to the fact that such systems feed on a constant flow of data, and that elimination mechanisms are not usually entirely watertight. Each of these issues is addressed below.

D.1 Depersonalization mechanisms

This first issue has not been previously explored by the Court or the literature. Article 12(2) of Directive (EU) 2016/681 instructs the PIUs to mask out some data elements six months after their collection, namely those “which could serve to identify directly the passenger to whom the PNR data relate.”¹¹³² Disclosing full PNR receipts then becomes conditional on verifying that two conditions have been met.

First, it must be “reasonably believed that it is necessary for the purposes referred to in point (b) of Article 6(2),”¹¹³³ that is, to respond “on a case-by-case basis, to a duly reasoned request based on sufficient grounds from the competent authorities to provide and process PNR data in specific cases for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime.”¹¹³⁴ Second, such a request must be accepted by “a judicial authority”¹¹³⁵ or by “another national authority competent under national law to verify whether the conditions for disclosure are met, subject to informing the data protection officer of the PIU and to an *ex-post* review by that data protection officer.”¹¹³⁶

These guarantees apparently suffice to protect data during any retention period. Yet, a closer look can prove otherwise. Already in 2011, the EDPS questioned any retention of data that allows individuals to be identified.¹¹³⁷ The supervisor suspected that, if PNR could be fully disclosed, this meant data were never entirely masked out.¹¹³⁸ It suggested that the proposal:

¹¹³² Article 12(2) of Directive (EU) 2016/681.

¹¹³³ Article 12(3)(a) of Directive (EU) 2016/681.

¹¹³⁴ Article 6(2)(b) of Directive (EU) 2016/681.

¹¹³⁵ Article 12(3)(b), point i, of Directive (EU) 2016/681.

¹¹³⁶ Article 12(3)(b), point ii, of Directive (EU) 2016/681.

¹¹³⁷ Opinion of the EDPS (OJ C 181, 22.6.2011), paragraph 43.

¹¹³⁸ *Idem*, paragraph 44.

[S]hould be reworded [to keep] the principle of real anonymisation with no way back to identifiable data, which means that no retro-active investigation should be allowed. These data could still — and solely — be used in order to serve general intelligence purposes based on the identification of terrorism and related crime patterns in migration flows.¹¹³⁹

That same year, the German Federal Council expressed a similar opinion, saying that, as data can be unmasked at any time, five years becomes disproportionately long from the stance of individual rights.¹¹⁴⁰ The Dutch Senate added that such anonymization mechanisms seemed inappropriate, as norms regarding payment data, for instance, were not impermeable.¹¹⁴¹

The depersonalization tools in PNR remain inadequate, five years after that proposal. There are two key problems worth mentioning. The first concerns the fact that not all data elements are depersonalized. The second, which will be addressed in the section on access rights by third parties, concerns the authorities who can authorize access requests from law enforcement.

Although Article 12(2) says that “all PNR data shall be depersonalised,”¹¹⁴² this is not true. This provision actually lists the elements that should be masked out, which are the:

(a) name(s), including the names of other passengers on the PNR and number of travellers on the PNR travelling together; (b) address and contact information; (c) all forms of payment information...which could serve to identify directly the passenger to whom the PNR relate or any other persons; (d) frequent flyer information; (e) general remarks to the extent that they contain any information which could serve to identify directly the passenger to whom the PNR relate; and (f) any API data that have been collected.¹¹⁴³

This leaves out some data that could still be used to identify passengers. Article 12 is silent, for example, on the “historical changes to the PNR,”¹¹⁴⁴ which may be essential to track criminal activities undertaken by law enforcement. So, the Directive is not only internally incongruent, it is not able to ensure full and secure anonymization during the lengthy data retention period.

The second problem that arises concerns the potential renewal of PNR receipts on a continuous basis, which leads to three chilling effects. These chilling effects are mainly related to the fear of constant surveillance that air passengers may experience due to the fact that their

¹¹³⁹ Opinion of the EDPS (OJ C 181, 22.6.2011), paragraph 45.

¹¹⁴⁰ Beschlussdes (6007/11), paragraphs 10 and 11.

¹¹⁴¹ Letter from René van der Linden, 1.

¹¹⁴² Article 12(2) of Directive (EU) 2016/681.

¹¹⁴³ They correspond to items 4, 5, 6, 8, 12, and 18 of Annex I of Directive (EU) 2016/681.

¹¹⁴⁴ Item 19 of Annex I of Directive (EU) 2016/681.

data may be retained for a very long, and perhaps unknown, period of time in the hands of many, and perhaps unknown, law enforcement agents.

D.2 Renewal of PNR receipts

The Directive obliges “Member States [to] ensure that the PNR data are deleted permanently upon expiry of the period”¹¹⁴⁵ of five years. Yet, this does not provide an answer as to what happens when passengers board new international flights before their previous receipts expire, something that is aggravated by the possibility of applying PNR to intra-EU flights.¹¹⁴⁶

Item 19 of Annex I indicates that the legislator may have thought about this, as PNR receipts should include “[a]ll historical changes to the PNR.”¹¹⁴⁷ Still, this fails to answer that question. It appears the Directive has provided the tools for member states to have permanent databases of constantly updated personal data of countless individuals from across the EU and overseas.

Every new PNR receipt transferred from carriers to the PIUs is added to the personal file of each air passenger. This creates a specific travel log. When data have been stored for 60 months, they are eliminated. But is the clock reset and data updated when a new flight is taken within those five years? It appears to be so. In that case, it seems the EU legislator has designed an automatic mechanism where PIUs are continually fed with a flow of personal data from all air passengers, and can subsequently provide other law enforcement with constantly updated personal information. From the onset, this can trigger, at least, three chilling effects.

D.2.1 First chilling effect

The first chilling effect is that data can be stored without deletion, or interruption, in databases available to law enforcement. If passengers take, at least, one international flight within those 60 months, a new complete PNR receipt is added to their travel logs and renewed data are available for criminal investigations for a new period of five years.

Every change to that personal information is registered. To take an international flight every five years is probably common for many people. In other words, this first chilling effect stems from PNR allowing for the continuous retention and processing by law enforcement of content

¹¹⁴⁵ Article 12(4) of Directive (EU) 2016/681.

¹¹⁴⁶ Article 2 of Directive (EU) 2016/681.

¹¹⁴⁷ Item 19 of Annex I of Directive (EU) 2016/681.

data of a very personal nature, belonging to all passengers of international flights crossing EU borders, for a very long period.

D.2.2 Second chilling effect

The second effect builds on the first. The depersonalization guarantees of the intra-EU PNR system are not adequate. Beyond the problems identified before, it must be recalled that these guarantees do not apply to the processing undertaken within the PIUs. Their personnel apparently have access to PNR receipts with no restrictions.

Article 6(2) lays out the purposes for which PIUs can process data. According to paragraph (c), they can analyze them “for the purpose of updating or creating new criteria to be used in the assessments carried out under point (b) of paragraph 3 in order to identify any persons who may be involved in a terrorist offence or serious crime.”¹¹⁴⁸ Point (b) of paragraph 3 talks about the processing of data “against pre-determined criteria”¹¹⁴⁹ to carry “out the assessment referred to in point (a) of paragraph 2.”¹¹⁵⁰ And point (a) of paragraph 2 addresses the first purpose for which PIUs can process data, namely to assess “passengers prior to their scheduled arrival in or departure from the Member State to identify persons who require further examination by the competent authorities.”¹¹⁵¹

Despite this confusing web of cross references, it is possible to distill the idea that PIUs create risk profiles whose building blocks (risk indicators) are determined by data collected from previous assessments. In a schematic way: PIUs receive data from carriers; the more passengers, the more data; the more data, the more and sharper risk factors to use in future assessments. So, when the cycle begins again, new passengers are scanned against more pre-determined criteria than previous passengers. Plus, their data will help to add new risk factors, or improve existing ones. The idea is not only to make risk factors more accurate. It is also about identifying “persons who were unsuspected of involvement in terrorist offences or serious crime prior to such an assessment.”¹¹⁵²

The goal is to broaden the scope and find unsuspected criminals, which can be a dangerous throttle as far as fundamental rights are concerned. The second chilling effect concerns the fact that the data that feed this system are, apparently, not depersonalized. Data controllers and

¹¹⁴⁸ Article 6(2)(c) of Directive (EU) 2016/681.

¹¹⁴⁹ Article 6(3)(b) of Directive (EU) 2016/681.

¹¹⁵⁰ Article 6(3) of Directive (EU) 2016/681.

¹¹⁵¹ Article 6(2)(a) of Directive (EU) 2016/681.

¹¹⁵² Recital (7) of Directive (EU) 2016/681.

processors in the PIUs, which are law enforcement authorities, are free to access personal content data for as long as they have them. And if the data of most passengers can stay in their databases on an endless loop, their privacy is undermined and the chances of misuse may be high, possibly for the rest of their lives.

Depersonalization mechanisms do not seem to apply to processing operations within the PIUs for two reasons. The first is that, when talking about accessing full PNR receipts upon expiry of the initial six months, Article 12(3) uses the term “disclosure”¹¹⁵³ of data. Disclosure means the exposure, or transfer, of information outside, to other authorities. Secondly, Article 12(3)(a) adds that disclosure depends on being “reasonably believed that it is necessary for the purposes referred to in point (b) of Article 6(2).”¹¹⁵⁴ This point (b) talks about transfers of data between PIUs, as well as to other competent authorities and to Europol.¹¹⁵⁵ While paragraphs (a) and (c) of Article 6(2) refer to the internal processing of data, paragraph (b) explicitly applies to their transfer.

Depersonalization guarantees therefore apply only to transfers of data, not to the processing which takes place inside the PIUs. Their operations undertaken under Articles 6(2)(a) and (c) are not affected by the masking of data. This means that PIUs can analyze PNR “for the purpose of updating or creating new criteria to be used”¹¹⁵⁶ in the “assessment of passengers prior to their scheduled arrival in or departure from the Member State”¹¹⁵⁷ with few limitations during the entire period for which they retain the data.

D.2.3 Third chilling effect

There is an additional chilling effect, which is the perpetuation of the feeling of surveillance, which was highlighted by Cruz Villalón when he wrote that the:

[C]ollection...and, above all, the retention...in huge databases, of...large quantities of data...establishes the conditions for surveillance which, although carried out only retrospectively when the data are used, [nonetheless] constitutes a permanent threat throughout the data retention period to the right of citizens of the Union to confidentiality in their private lives. The vague feeling of surveillance created raises very acutely the question of the data retention period.¹¹⁵⁸

¹¹⁵³ Article 12(3) of Directive (EU) 2016/681.

¹¹⁵⁴ Article 12(3)(a) of Directive (EU) 2016/681.

¹¹⁵⁵ Article 6(2)(b) of Directive (EU) 2016/681.

¹¹⁵⁶ Article 6(2)(c) of Directive (EU) 2016/681.

¹¹⁵⁷ Article 6(2)(a) of Directive (EU) 2016/681.

¹¹⁵⁸ Opinion of AG Cruz Villalón, paragraph 72.

The feeling he was talking about becomes more ominous the longer the data are retained. And, in the case of PNR, this type of surveillance is not undertaken only in a retrospective manner, but can take place before and during the flight. Article 6(2) reads that PIUs “shall process PNR data [to carry out assessments] prior to their scheduled arrival in or departure from the Member State.”¹¹⁵⁹ Passengers might be aware of being monitored, but they do not know the details of the interference with their rights.

Most passengers are not entirely conscious of PNR. Yet, this does not diminish its iniquity. It has been demonstrated that, in practice, data can be held for a passenger’s entire life, with no interruption or deletion, and regardless of criminal records. Besides, whenever they reserve new flights, data are automatically updated, even if they do not board. And the passing of time does not affect the quality of the data in typical ways. Time actually increases the monitoring capacities of authorities, with little effort from their end. Furthermore, as there are no objective criteria limiting processing within and, to an extent, outside of the PIUs, the threshold of five years may be little more than a regulatory sham.

The fear expressed by the AG acquires a new tone with PNR. This fear was also expressed by the CJEU when claiming that so much information being collected and processed without the data subjects being aware may lead to the perception that their lives are subject to continuous monitoring.¹¹⁶⁰ Is this only a mere feeling in the case of the intra-EU PNR system?

The Directive’s interference with fundamental rights is not limited to that which is strictly necessary, with regard to the data retention period. Not only are there no criteria explaining how its length is limited, there is also no differentiation between the treatment of data from suspect passengers and that of data from innocent passengers. Plus, the irreversible destruction of data is not guaranteed and there are no adequate rules on depersonalization, or on the renewal of PNR receipts. The CJEU might need to reconsider whether the intricacy of criminal investigations provides sufficient grounds to claim that a retention period of five years “does not exceed the limits of what is strictly necessary for the purposes of combating terrorism and serious transnational crime.”¹¹⁶¹

The final aspect that is going to be discussed regarding the proportionality of the PNR Directive is about access rights and the third parties who can handle data. As with the previous sections, this next section is divided into subsections that correspond to the criteria which the

¹¹⁵⁹ Article 6(2)(a) of Directive (EU) 2016/681.

¹¹⁶⁰ Joined cases C-293/12 and C-594/12, paragraph 37.

¹¹⁶¹ Opinion 1/15, paragraphs 205 and 209.

CJEU and scholars have deemed relevant in assessing whether access to data is sufficiently limited to justify the interference with fundamental rights.

6.2.3 Third parties with access rights

A. Public entities

A.1 Competent authorities

Article 7 of Directive (EU) 2016/681 is more detailed than Article 4 of Directive 2006/24/EC regarding the authorities who have access rights. The latter gave a wide margin of discretion to member states and its relevant problems have been addressed in the previous part of this chapter. The most pertinent remark of the Court was that it did not table objective standards to limit access to and processing of data by law enforcement agencies.¹¹⁶²

Article 7 leaves member states free to “adopt a list of the competent authorities entitled to request or receive PNR data.”¹¹⁶³ Yet there are conditions on access:¹¹⁶⁴ authorities must be “competent for the prevention, detection, investigation or prosecution of terrorist offences or serious crime,”¹¹⁶⁵ and data can only be used for such purposes.¹¹⁶⁶ Besides, Article 7(3) requires member states to notify the Commission if they alter the lists of authorities with access.

Despite this apparent tightness, the interference with privacy and data protection goes beyond the strictly necessary. The current drafting of the Directive does not sufficiently limit access and processing operations, which could potentially lead to violations of the CFREU. It is more robust than the data retention Directive, which had no limits at all and presented no guidelines to define them.¹¹⁶⁷ But the PNR system is still not good enough.

This happens for three main reasons. First, Article 7(5) opens the door for law enforcement other than those mentioned in the lists referred to in number 1 to access data, thus circumventing all mechanisms to limit the authorities with access rights. Second, the Directive is not clear regarding the personnel authorized to process the information. Third, the prior review for requests to access PNR receipts does not meet the criteria tabled by the CJEU. Before

¹¹⁶² Joined cases C-293/12 and C-594/12, paragraph 60.

¹¹⁶³ Article 7(1) of Directive (EU) 2016/681.

¹¹⁶⁴ Notably, in Article 6(2)(b) of Directive (EU) 2016/681.

¹¹⁶⁵ Article 7(2) of Directive (EU) 2016/681.

¹¹⁶⁶ Article 7(1) of Directive (EU) 2016/681, *in fine*.

¹¹⁶⁷ Joined cases C-293/12 and C-594/12, paragraph 60.

addressing these reasons, however, there is a broader concern stemming from recent jurisprudence that might raise some questions regarding the pre-emptive logic of data transfers in the PNR system, and of all data retention mechanisms that depend on the collection of data by private actors.

A.1.1 A broader concern

In the *Tele2* case, the Court adopted a rather strong view on the limits of cooperation between private and public actors on data transfers for criminal investigation purposes. A view which seems to go directly against the very functioning of PNR.

The judges wrote that, in principle, private actors can grant public bodies access, “in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime.”¹¹⁶⁸ The only exception where “access to the data of other persons might also be granted [is when] there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating...terrorist activities [threatening, for example,] vital national security, defence or public security interests.”¹¹⁶⁹

This would apparently mean that, except in duly justified cases, competent authorities, at least regarding the processing of electronic communications data, can never access, or successfully require access to, data subjects’ personal information in an indiscriminate and blanket manner. This seems a clear benchmark which implies that national laws, and certainly EU law as well, must not provide for generalized access by public entities for large-scale surveillance purposes.¹¹⁷⁰ Based on years of jurisprudence reiterating the need for laying out conditions on public access to private data, this position of the Court is a good sign for those advocating in favor of targeted retention practices.

However, in *La Quadrature du Net*, an even more recent case, the Court took a step forward and a step back in this regard. The step forward arises from the fact that it laid out additional criteria to further narrow access by public entities to private data. It wrote that the CFREU does not, in principle, preclude measures permitting authorities to “retain traffic and location

¹¹⁶⁸ Joined cases C-203/15 and C-698/15, paragraph 119 (which mentions the ECtHR case *Roman Zakharov v Russia*, 4 December 2015 (47143/06), paragraph 260).

¹¹⁶⁹ *Ibidem*. See, analogically, paragraph 188.

¹¹⁷⁰ Possibly in an attempt to make a sharp turn in the slippery slope that policies and measures on criminal procedure law have been undertaking in recent decades of generalizing suspicion and setting aside the need for previous warrants and mandates to collect big data and interfere with the privacy and fundamental rights of large troves of the population.

data...for a limited period of time, as long as there are sufficiently solid grounds for considering that the Member State concerned is confronted with a serious threat...to national security which is shown to be genuine and present or foreseeable.”¹¹⁷¹ And it added that, even if there is apparently no connection of the affected data subjects with those threats, their objective existence “is, in itself, capable of establishing that connection”¹¹⁷² and, thus, justify access to data. It likewise stated that the “retention [of data] cannot be systematic in nature.”¹¹⁷³

Although the formulation could be clearer, it seems that, for the CJEU, beyond being allowed only to access the information of relevant persons, law enforcement can also only do so for a limited period of time and only at particular moments, when there is strong evidence of a serious, genuine, and present or foreseeable threat to national security. This is quite a heavy set of standards which may well mean the beginning of the end for mass-surveillance practices by public entities outside very specific cases.

Yet, when laying out these other criteria, the judges did not mention that only the data of concrete individuals could be retained. On the contrary, they focused on the fact that EU law and the CFREU do not, in principle, preclude measures permitting authorities to “retain traffic and location data of all users of electronic communications systems.”¹¹⁷⁴ This is the step backwards mentioned above. It could reasonably be hoped that, while talking about the same EU law provision and similar measures enacted by the member states pursuant to it, the case law would show a higher degree of consistency and predictability. As things stand, it is uncertain whether blanket data retention schemes are, indeed, lawful, or not.

This discussion, relevant though it is, is beyond the scope of this research, and this section in particular. The pressing concern, for now, is whether the Court considers that such limiting criteria should apply to all big data retention-based systems or, on the contrary, only to the specific case of telecommunications operators collecting data from their clients and supplying them on demand for investigatory purposes, after a justified request, on a case-by-case basis.

If the former were true and the judges were thinking that access to and the processing of data by law enforcement should be thus limited in all systems, this would strongly reinforce an

¹¹⁷¹ Joined cases C-511/18, C-512/18 and C-520/18, paragraph 137.

¹¹⁷² *Ibidem*.

¹¹⁷³ *Idem*, paragraph 138. In paragraph 142, the CJEU went as far as saying that, “[i] view of the sensitive nature of the information that traffic and location data may provide...it is necessary, within a democratic society, that retention be the exception and not the rule...and that the data not be retained systematically and continuously. That conclusion applies even having regard to the objectives of combating serious crime and preventing serious threats to public security and to the importance to be attached to them.” As mentioned before, applying this reasoning directly to the PNR system would arguably mean its invalidity. The reading of the jurisprudence is, therefore, somewhat narrow to shield the analysis from criticism of being vague, broad, or over-exploratory.

¹¹⁷⁴ Joined cases C-511/18, C-512/18 and C-520/18, paragraph 137.

argument in favor of the invalidity of the PNR Directive. In fact, PNR is built upon the continuous and systematic collection of passenger data by competent authorities (PIUs) which are supplied by private actors (air carriers). This private-to-public cooperation, through the so-called push method, is not incidental, but a critical aspect of the system; one of its very initial processing stages.¹¹⁷⁵ It not only affects all passengers but data are collected regardless of any serious, genuine, and present or foreseeable threat to national security. Plus, it has been established that the period of time during which PNR are retained is not limited to that which is strictly necessary. The intra-EU system fails to meet all criteria.

But is this what the Court really intended? It may be too soon to answer in the affirmative. As such, this concern is not relied on here as one of the specific reasons why the Directive does not appear to be sufficiently limited in terms of access to data. It does not seem reasonable to assume that the CJEU would want to bluntly apply these standards to all data retention systems.

For this reason, it will not be argued that the intra-EU PNR is invalid, from the perspective of access to data by law enforcement, because it allows, as a general rule, for the indiscriminate and continuous granting of access to the data of air passengers by carriers for the purposes of fighting terrorism and serious crime. It is true that the extensive and continuous access to, storing, and availability of data are features that raise questions and possibly render the Directive disproportionate. But, for now, it is time to explore three specific reasons why it can be safely argued that the PNR system is not sufficiently tight, going beyond that which is strictly necessary in terms of access by law enforcement agencies to passenger data.

A.1.2 Opening of the system

Article 7(4) says that “[t]he PNR data and the result of processing those data received by the PIU may be further processed by the competent authorities of the Member States only for the specific purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious crime.”¹¹⁷⁶ It is a clear, straightforward, and objective provision. Above all, it is limited to that which is necessary to attain the purposes of the system. However, Article 7(5) adds that “[p]aragraph 4 shall be without prejudice to national law enforcement or judicial powers where

¹¹⁷⁵ Vide Articles 1(a), 3, paragraph (7), 4(2)(a), 6(1), 8, 12(1), and 16(1) and (2), as well as Annex I, of Directive (EU) 2016/681.

¹¹⁷⁶ Article 7(4) of Directive (EU) 2016/681.

other offences, or indications thereof, are detected in the course of enforcement action further to such processing.”¹¹⁷⁷

This defeats the tight logic of Article 7, if not of the whole Directive, in terms of limiting data processing and access rights to “the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime.”¹¹⁷⁸ Article 7(5) admits that other law enforcement can access PNR and allows for the investigation of other types of crime.

On the one hand, it mentions “national law enforcement or judicial powers,”¹¹⁷⁹ instead of “competent authorities.”¹¹⁸⁰ So, it assumes data can be transferred to other entities beyond those chosen by the member states to be “entitled to request or receive PNR data.”¹¹⁸¹ It provides the member states with a wide margin of discretion, with no objective criteria limiting the scope of this discretion. The idea of having lists of entities with access rights, and the legal certainty and security this brings, are clearly undermined.

They are also undermined because that provision allows PNR data, which should be processed “only for the specific purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious crime,”¹¹⁸² to be processed to fight “other offences.”¹¹⁸³ Article 7(4), many other provisions,¹¹⁸⁴ and Annex II, which lists the offenses that can be investigated, are thus deprived of most of their legal relevance.

This incongruence is preoccupying. With this opening, the Directive undermines the principle of purpose limitation, as well as any attempt to achieve legal security and certainty. Article 7 opens access to PNR data to entities, and for purposes, outside the logic and control of the Directive, and, perhaps, EU secondary law more broadly. It presents access limits, but immediately allows the member states to surpass them.

While fighting other criminal offenses makes sense in the logic of this legislation, it does not serve its specific and precise objectives.¹¹⁸⁵ There is no concrete standard¹¹⁸⁶ to fully limit access to, and use of, PNR data, thereby ensuring that the interference with fundamental rights does not go beyond that which is strictly necessary. Because of this exception, the criticism levelled against the data retention Directive applies also to the intra-EU PNR. It similarly does

¹¹⁷⁷ Article 7(5) of Directive (EU) 2016/681.

¹¹⁷⁸ Articles 7(1), *in fine*, 7(2), and 7(4) of Directive (EU) 2016/681.

¹¹⁷⁹ Article 7(5) of Directive (EU) 2016/681.

¹¹⁸⁰ Article 7(4) of Directive (EU) 2016/681.

¹¹⁸¹ Article 7(1) of Directive (EU) 2016/681.

¹¹⁸² Article 7(4) of Directive (EU) 2016/681.

¹¹⁸³ Article 7(5) of Directive (EU) 2016/681.

¹¹⁸⁴ Namely, Articles 1(2), 6(2), 7(1), 11(1)(b) and (c), 12(3)(a) and (4), and 16(1) and (2) of Directive (EU) 2016/681.

¹¹⁸⁵ Enerstvedt, 2017: 191.

¹¹⁸⁶ Joined cases C-293/12 and C-594/12, paragraph 60.

“not expressly provide that that access and the subsequent use of the data in question [are] strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto.”¹¹⁸⁷

A.1.3 Authorized personnel

The CJEU added that Directive 2006/24/EC likewise failed to provide concrete criteria to limit the people accredited to process the collected information.¹¹⁸⁸ It does not require EU law to define exactly the number of people with access rights. This is impossible to do. The key here is that there must be a criterion to limit the number of such persons.

The PNR Directive is silent on this matter. It tables no criteria that could be used to ascertain, or limit, the number of people working in the PIUs, or in other authorities. A proposal could be to limit access by ranking levels, or to specify that only people essential to the conduct of ongoing investigations be permitted to handle PNR receipts. As it stands, it is entirely up to the member states to decide, and they may end up not setting sufficiently high access requirements. This jeopardizes the rights to privacy and data protection for all those whose data may circulate through too many pairs of hands.

The only reference to access levels is in Article 13. Article 13(5) states that “Member States shall ensure that the PIUs maintain documentation relating to all processing systems and procedures under their responsibility.”¹¹⁸⁹ Such documentation must contain “the name and contact details of the organisation and personnel in the PIU entrusted with the processing of the PNR data and the different levels of access authorisation.”¹¹⁹⁰ Yet, this is a procedural norm, aimed at ensuring PIUs record the trail of access to databases. It does not oblige the member states to define a hierarchy concerning different access levels and authorization procedures within the PIUs. Access may still be provided well beyond the rationale present in the case law.

Defining access levels must be a shared responsibility. It does not suffice to have member states freely define access levels, or other access conditions. The PNR Directive similarly fails to meet the requirements set by the CJEU in this regard.

¹¹⁸⁷ Joined cases C-293/12 and C-594/12, paragraph 61.

¹¹⁸⁸ *Idem*, paragraph 62.

¹¹⁸⁹ Article 13(5) of Directive (EU) 2016/681.

¹¹⁹⁰ Article 13(5)(a) of Directive (EU) 2016/681.

A.1.4 Prior review

There is another reason why the norms concerning competent authorities with access rights to data cannot be considered to be limited to that which is strictly necessary. It has to do with the mechanisms of prior review, which the Court considers a very relevant feature of data retention systems. In *Digital Rights Ireland*, it commented that:

[A]ccess by the competent national authorities to the data [was] not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions.¹¹⁹¹

It reinforced this position in *Opinion 1/15*, claiming that prior review “by a court or independent administrative body...should [be] a general rule”¹¹⁹² for third-party access and use of data, except in urgent situations. Although the Court did not elaborate further, these paragraphs are paramount to big data processing operations.

The principle of prior review, which is part and parcel of the logic of traditional judicial mandates and detention orders, serves the principle of good administration and is of key importance in procedural law and criminal investigations. It emerges strengthened by the CJEU’s case law. It is clear that law enforcement authorities must request permission from a judicial power, or otherwise independent administrative authority, to have access to PNR. This prevents the issuing and acceptance of requests that are not sufficiently supported by evidence of criminal actions. It shields the privacy of air passengers. It is likewise an imperative of fair processing and, therefore, of the right to data protection.

Prior review is a foundational value in security and criminal law. It gives power to judicial, or quasi-judicial bodies, against the adoption of arbitrary decisions by law enforcement. It is thus of particular relevance in procedures involving big data, and in which the information is processed in increasingly faster and more automatized ways. It is, however, a principle which the legislator tried to circumvent in *Directive 2006/24/EC*, in the *EU-Canada PNR Agreement*, and in *Directive (EU) 2016/681*.

From the onset, the depersonalization tool in *Article 12* appears sufficient to comply with the requirement of prior review. Six months after collection, “disclosure of the full PNR data

¹¹⁹¹ Joined cases C-293/12 and C-594/12, paragraph 62.

¹¹⁹² *Opinion 1/15*, paragraph 202.

shall be permitted only”¹¹⁹³ when it is “reasonably believed [to be] necessary”¹¹⁹⁴ and after “a duly reasoned request based on sufficient grounds from the competent authorities...in specific cases for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime.”¹¹⁹⁵ Such requests must be “approved by: (i) a judicial authority; or (ii) another national authority competent under national law to verify whether the conditions for disclosure are met, subject to informing the data protection officer of the PIU and to an *ex-post* review by that data protection officer.”¹¹⁹⁶

A close look reveals deep problems with these provisions. The first is that not all data are masked out. This has been addressed above in the section on depersonalization. The second problem stems from the fact that prior review in PNR is only mandatory six months after the collection of the data. Finally, the Directive is also flawed regarding the authorities competent to authorize access requests.

i) Moment of review

Article 12(2) says that “[u]pon expiry of a period of six months after the transfer of the PNR data [from air carriers to PIUs], all PNR data shall be depersonalised.”¹¹⁹⁷ And Article 12(3) adds that law enforcement shall be authorized to access full PNR receipts following prior review “[u]pon expiry of [that] period of six months.”¹¹⁹⁸

The legislator has not explained why depersonalization, and, consequently, prior review, take place only six months after collection. Recital (37) holds that the “scope of this Directive is as limited as possible since...it provides for the data to be depersonalised through masking out of data elements after an initial period of six months.”¹¹⁹⁹ Yet, there are no reasons justifying this waiting period, which seems arbitrary.

Until this period expires, the data can be accessed upon request but prior review is not necessary. This means that, during those first six months, the period during which it is likely that data will be requested most frequently, a key mechanism to prevent abusive access and processing is purposefully set aside in the Directive.

¹¹⁹³ Article 12(3) of Directive (EU) 2016/681.

¹¹⁹⁴ Article 12(3)(a) of Directive (EU) 2016/681.

¹¹⁹⁵ Article 6(2)(b) of Directive (EU) 2016/681.

¹¹⁹⁶ Article 12(3)(b) of Directive (EU) 2016/681.

¹¹⁹⁷ Article 12(2) of Directive (EU) 2016/681.

¹¹⁹⁸ Article 12(3) of Directive (EU) 2016/681.

¹¹⁹⁹ Recital (37) of Directive (EU) 2016/681.

The case law makes no mention of temporal gaps related to prior review. As such, the Directive is not limited to that which is strictly necessary, as it allows for law enforcement to access data stored by the PIUs without having to ask for permission from courts or independent administrative authorities, during the first months of the retention period.

The legislator yet again seems to have ignored the CJEU. It could simply have made prior review mandatory for all requests. In fact, without the six months' gap, the conditions on access laid out in Article 6(2)(b), read together with the depersonalization and prior review set in Article 12, would meet the demands of the jurisprudence.

This leads to another discussion. It is easy to resolve the matter of data transfers from the PIUs to other competent authorities. Provided all requests are subject to prior review, the balance between the purposes of the system and respect for the fundamental rights of passengers appears to be maintained in line with the proportionality principle. Yet, what about access inside the PIUs?

The Directive assumes that masking out data does not apply to internal operations. This evokes the second chilling effect stemming from the renewal of PNR receipts, which consists of allowing data to be freely accessible to the PIUs and their personnel for the full length of the retention period. It seems that, to maintain the rights of passengers while allowing law enforcement to search through the data, depersonalization and prior review should also apply to processing which takes place within the PIUs.

This would not require considerable changes to the current system, or a gap of six months. Article 6(2) foresees that the PIUs will process PNR to carry “out an assessment of passengers prior to their scheduled arrival in or departure from the Member State”¹²⁰⁰ and to analyze “data for the purpose of updating or creating new criteria...in order to identify any persons who may be involved in a terrorist offence or serious crime.”¹²⁰¹ These provisions are clear with respect to what the PIUs should do. Therefore, a tool that would pay attention to the CJEU's remarks, protect fundamental rights, and allow the system to keep functioning, could be to instruct the PIUs to store data immediately after they have processed them and assessed passengers. Once they had done so, and no longer needed access to those elements for ongoing investigations or other immediate purposes, the data should be fully depersonalized. Subsequently, their use and disclosure in and outside of the PIUs, would have to be subject to prior review.

This would make all access to depersonalized data dependent on prior review, turning it into a feature embedded by design in the system. However, it must be understood without prejudice

¹²⁰⁰ Article 6(2)(a) of Directive (EU) 2016/681.

¹²⁰¹ Article 6(2)(c) of Directive (EU) 2016/681.

to the remarks made, for instance, about the excessive collection of data, or the need to limit the retention period.

ii) Competent authorities

While Article 12(3)(b), point i, says that disclosure of full PNR receipts must be approved by a judicial authority, its point ii mentions that, in the alternative, approval can come from any other “authority competent under national law to verify whether the conditions for disclosure are met, subject to informing the data protection officer of the PIU and to an *ex-post* review by that data protection officer.”¹²⁰² This is different from making access depend on “prior review carried out by...an independent administrative body.”¹²⁰³

With such wording, member states can make competent authorities who depend on ministries, or other political offices, approve access requests. In the words of Saulnier-Cassia, it truly seems that anonymity in PNR “n’est donc qu’un leurre.”¹²⁰⁴

This opening facilitates third party-access to PNR authorized by non-independent and non-judicial authorities, and the last part of that provision is insufficient to overcome this setback. Although the inclusion of DPOs has been hailed as a key guarantee to shield air passengers’ rights,¹²⁰⁵ their competences are limited here. For one thing, nothing in Article 5, which regulates them,¹²⁰⁶ appears to indicate that they can prevent abusive disclosure of PNR receipts. For another, an *ex-post* review is insufficient from the angle of data subjects. It does not prevent third parties from accessing the data, or address the possible consequences that arise from this interference. Once data start circulating, it is extremely hard, if not impossible, to extract all of them from the system. This is quite worrying if, for instance, the request for access comes from an authority located outside the Union.

Contrary to what recital (38) claims, the “Directive does...go beyond what is necessary in order to achieve [its] objectives.”¹²⁰⁷ As such, it should be considered that, by adopting PNR,

¹²⁰² Article 12(3)(b), point ii, of Directive (EU) 2016/681.

¹²⁰³ Joined cases C-293/12 and C-594/12, paragraph 62. See also Opinion 1/15, paragraph 202.

¹²⁰⁴ Saulnier-Cassia, 2017: 218.

¹²⁰⁵ See Villani, 2018: 902, Carpanelli & Lazzerini, 2017: 395, or Di Matteo, 2017: 231.

¹²⁰⁶ It reads that “1. The PIU shall appoint a data protection officer responsible for monitoring the processing of PNR data and implementing relevant safeguards. 2. Member States shall provide data protection officers with the means to perform their duties and tasks in accordance with this Article effectively and independently. 3. Member States shall ensure that a data subject has the right to contact the data protection officer, as a single point of contact, on all issues relating to the processing of that data subject’s PNR data.”

¹²⁰⁷ Recital (38) of Directive (EU) 2016/681.

the EU legislator “exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter.”¹²⁰⁸

A.2 Third countries

Europol¹²⁰⁹ and third countries¹²¹⁰ can also request access to PNR receipts. There seems to be no relevant problem with Europol retrieving such data, mainly due to the strict conditions imposed by the Directive.

David Lowe has, curiously, suggested that member states should require Europol to review access requests in certain circumstances, particularly from third countries.¹²¹¹ This idea could be discussed in future reviews.¹²¹² However, Lowe is unclear on whether this should be mandatory or optional, and how it could be applied, particularly in terms of time efficiency viz. urgent requests. Article 11(2) says that, in exceptional circumstances and under strict criteria, PIUs can send data to third countries without prior authorization from the competent authorities of the member states. Two such criteria are that these transfers serve to tackle an “(a) actual threat...and [that] (b) prior consent cannot be obtained in good time.”¹²¹³ Lowe does not engage with these norms, thus failing to test his suggestion, and potentially jeopardizing the argument.

Article 11 allows for transfers to third countries on “a case-by-case basis”¹²¹⁴ and in accordance with certain requirements. One of these requirements is that transfers among third countries can only take place if the third country which originally received data from a member state “agrees to transfer the data to another third country only where it is strictly necessary for the purposes of this Directive...and only with the express authorisation of that Member State.”¹²¹⁵ These are robust obligations, though they give member states considerable leeway to make decisions about data transfers. In any case, given the way in which Article 11 is written, the legislator conveys the idea that transfers from member states to third countries should be exceptional. Hence, transfers between third countries should be relatively uncommon.

As it stands, Article 11 appears more watertight than Article 19 of the EU-Canada Agreement. This was criticized by the Court for allowing for the disclosure of data to other

¹²⁰⁸ Joined cases C-293/12 and C-594/12, paragraph 69.

¹²⁰⁹ Article 10 of Directive (EU) 2016/681.

¹²¹⁰ Article 11 of Directive (EU) 2016/681.

¹²¹¹ Lowe, 2016: 878.

¹²¹² See Article 19 of Directive (EU) 2016/681.

¹²¹³ Articles 11(2)(a) and (b) of Directive (EU) 2016/681.

¹²¹⁴ Article 11(1) of Directive (EU) 2016/681.

¹²¹⁵ Article 11(1)(c) of Directive (EU) 2016/681.

third countries without there being a similar agreement between them and the Union, or an adequacy decision from the Commission ensuring that they adequately protected data according to EU law standards and mentioning all entities that could receive PNR receipts.¹²¹⁶ Article 19 could allow data to escape the control of EU law and give rise to an interference with individual rights, beyond that which was necessary to fulfill the Agreement's objectives.¹²¹⁷

The intra-EU PNR manages to avoid this criticism up to a point. Article 11(1)(a) says that transfers overseas can only happen if “the conditions laid down in Article 13 of Framework Decision 2008/977/JHA are met.”¹²¹⁸ This guarantees that the receiving “third State...ensures an adequate level of protection for the intended data processing.”¹²¹⁹ That Framework Decision was repealed by Directive (EU) 2016/680 but the obligation has remained. Its Article 35(1)(d) requires, as a general principle for data transfers, that “the Commission has adopted an adequacy decision...or, in the absence of such a decision, [that] appropriate safeguards have been provided...or, in [their] absence [that] derogations for specific situations apply.”¹²²⁰

Alas, this is flawed for three reasons. First, since Article 35(1)(d) of Directive (EU) 2016/680 has a considerably broader scope than Article 13 of Framework Decision 2008/977/JHA, it is less clearly determined when third countries can be deemed to be ensuring an adequate level of data protection. Plus, it is not clear which derogations apply in the case of PNR, which undermines the principles of legal certainty and security.

Second, Article 11 of the PNR Directive does not explicitly say that third countries which receive data from other third countries must guarantee an adequate level of protection. It could be argued that, if one of the conditions for having member states transfer PNR data abroad is that receiving third countries ensure an adequate level of protection, these non-member states should likewise send data only to third countries fulfilling this criterion. Yet, this is not explicit in the provision. As stated above, assessing whether third countries provide for the necessary conditions to protect data seems to be at the discretion of the member states. It is doubtful whether the CJEU would find this to be an adequate way to ensure that the data remain secure once they leave the Union. The level of control exerted by EU law is very thin in these situations, and it is not possible to avow that transfers will be made only in the case of a previous international agreement or an adequacy decision issued by the Commission.¹²²¹

¹²¹⁶ Opinion 1/15, paragraph 214.

¹²¹⁷ *Idem*, paragraph 215.

¹²¹⁸ Article 11(1)(a) of Directive (EU) 2016/681.

¹²¹⁹ Article 13(1)(d) of Framework Decision 2008/977/JHA.

¹²²⁰ Article 35(1)(d) of Directive (EU) 2016/680.

¹²²¹ Opinion 1/15, paragraph 214.

A final reason for considering that transfers of data to third countries are not limited to that which is strictly necessary, is that Article 11(2) allows for transfers without prior consent of the member states in “exceptional circumstances.”¹²²² It is difficult to know whether this applies to transfers between third countries, or also from member states to non-member states. The issue is that, at this stage and with technologies capable of processing data at an unprecedented scale, it is not possible to ensure that these openings will not present unnecessary risks for the privacy of passengers and the integrity, safety, and secrecy of data. They do not come accompanied by safeguards that could be invoked quickly in the event of abusive transfers.

The problems identified here seem to dilute the control over data exerted by member states and the EU. The provisions mentioned should be removed, or redrafted, as they are not limited to that which is strictly necessary in light of the Directive’s objectives.

There is another issue on access to PNR, which concerns the responsibilities of private actors towards the data. This is sometimes overlooked by scholars and even institutional actors, particularly because PNR legislation tends to be silent in this regard. Yet, the Court has been quite clear in stressing that carriers and non-carriers alike should protect data in a satisfactory way and should provide for the elimination of records from their databases.

B. Private actors

The judges focused on the right to data protection when discussing the provisions of Directive 2006/24/EC enabling private actors to process and transfer information. They found that the legislation did not ensure a sufficient level of data safety.¹²²³

The PNR Directive is not detailed on the processing undertaken by carriers, instead focusing on the activities of competent authorities. As such, there are but two aspects meriting discussion. The first is the fact that they may take economic considerations into account when implementing data security mechanisms. The second is the lack of norms providing for the elimination of the information collected when the retention period expires.

In the case *La Quadrature du Net*, the judges discussed the interference provoked with fundamental rights stemming from having private actors automatically analyze traffic and location data.¹²²⁴ A key conclusion is that they apply the same principles, and worry about the same issues, regardless of the nature of the entity undertaking the automated analysis. The items

¹²²² Article 11(2) of Directive (EU) 2016/681.

¹²²³ Joined cases C-293/12 and C-594/12, paragraph 67.

¹²²⁴ Joined cases C-511/18, C-512/18 and C-520/18, paragraphs 172 ff.

and criteria mentioned by the CJEU are the same as have been used throughout this thesis concerning the processing of data by law enforcement and what constitutes a serious interference from the point of view of the proportionality principle. In fact, the judges often refer to previous paragraphs in this new case law to avoid repetition. Therefore, considering that the PNR Directive purposefully does not regulate processing undertaken by carriers, which falls under the scope of other instruments,¹²²⁵ it seems unnecessary to discuss this topic beyond the two issues referred to above.

B.1 Economic considerations

The data retention Directive allowed private actors to consider economic factors when setting their security levels. This was because Article 7 read that compliance with “data security principles with respect to data retained in accordance with [the] Directive [was without] prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC.”¹²²⁶ Articles 4(1) of Directive 2002/58/EC and 17(1), 2nd paragraph, of Directive 95/46/EC stated that all appropriate technical and organizational measures to protect data should observe the “state of the art and the cost of their implementation.”¹²²⁷

The silence of the data retention Directive made it possible to interpret its Article 7 as a doorway for allowing economic considerations to influence the decisions of providers when implementing data protection safeguards. This made the CJEU fear that private actors would try to cut down on costs by applying less protective data systems, as this legal opening would allow them to lawfully lower the level of data protection.

The PNR Directive is also silent. Still, Articles 13(3) and 21(2) render the GDPR applicable to processing undertaken by carriers, and Article 25(1) of the GDPR says that “the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures...[t]aking into account the state of the art [and] the cost of implementation.”¹²²⁸

These references lure PNR into the same trap as the data retention Directive. In fact, the GDPR partially copies Directives 95/46/EC and 2002/58/EC. In both cases, references to other legislation make the data retention and PNR Directives unable to ensure that private actors

¹²²⁵ Namely, the GDPR.

¹²²⁶ Article 7 of Directive 2006/24/EC.

¹²²⁷ Articles 4(1) of Directive 2002/58/EC and 17(1), 2nd paragraph, of Directive 95/46/EC.

¹²²⁸ Article 25(1) of Regulation (EU) 2016/679. This is repeated in Article 32(1), which regulates the security of processing.

employ sufficient technological and administrative tools to keep data safe, because they may consider economic factors when they define and implement these security mechanisms.¹²²⁹

The intra-EU PNR system thereby creates a risk for fundamental rights, because data are not entirely safe while being processed and retained by carriers. The interference they provoke in the lives of air passengers is not limited to that which is strictly necessary.

B.2 Irreversible destruction of data

Article 7, paragraph (d), of Directive 2006/24/EC determined that “the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention.”¹²³⁰ The exception between commas led the CJEU to doubt the data retention Directive provided for the permanent elimination of the information retained.¹²³¹

Article 8 of the PNR Directive does not talk about the disposal of data. This is probably because carriers are free to use them for purposes beyond the scope of the Directive. The data that are transferred to the PIUs are, in fact, the same that are “already collected...in the normal course of their business.”¹²³² However, this creates a problem.

Article 8(3) says that transfers shall take place: “(a) 24 to 48 hours before the scheduled flight departure time; and (b) immediately after flight closure, that is once the passengers have boarded the aircraft in preparation for departure and it is no longer possible for passengers to board or leave.”¹²³³ Yet, Article 8(5) adds that:

Where access to PNR data is necessary to respond to a specific and actual threat related to terrorist offences or serious crime, air carriers shall, on a case by case basis, transfer PNR data at other points in time than those mentioned in paragraph 3, upon request from a PIU in accordance with national law.¹²³⁴

This means that carriers must retain data for an indefinite period of time while waiting for PIUs to request them. Though this should happen “on a case by case basis,”¹²³⁵ neither the carriers nor the PIUs know when, or if, such cases will occur. In practice, PNR data must be kept with no depersonalization, or other data protection guarantees expressly foreseen in the

¹²²⁹ Joined cases C-293/12 and C-594/12, paragraph 67.

¹²³⁰ Article 7, paragraph (d), of Directive 2006/24/EC.

¹²³¹ Joined cases C-293/12 and C-594/12, paragraph 67.

¹²³² Article 8(1) of Directive (EU) 2016/681.

¹²³³ Articles 8(3)(a) and (b) of Directive (EU) 2016/681.

¹²³⁴ Article 8(5) of Directive (EU) 2016/681.

¹²³⁵ *Idem*.

Directive, for an indeterminate period, in the databases of private actors. This evades relevant safeguards, and undermines any expectation of legal security or certainty. It goes directly against what the CJEU recently emphasized in the case *La Quadrature du Net*. The judges argued that, on the one hand, the retention of information by private actors, under the instruction of public agencies, “cannot exceed a foreseeable period of time.”¹²³⁶ On the other, that “data must, in principle, be erased or made anonymous, depending on the circumstances, at the end of the statutory periods within which that data must be processed and stored in accordance with...national provisions.”¹²³⁷ While the case was about national legislation transposing Directive 2002/58/EC, in line with *Digital Rights Ireland*, it can be said that EU law should also contain references to such deletion or depersonalization procedures, or, at least, foresee obligations for member states to enact norms in that regard.

Article 8(5) of Directive (EU) 2016/681 serves a parallel goal, which was enshrined in that jurisprudence too, when the judges tried to ensure that:

[D]uring...processing and storage, situations may arise in which it becomes necessary [for private actors] to retain that data after those time periods have ended in order to shed light on serious criminal offences or acts adversely affecting national security; this is the case both in situations where those offences or acts having adverse effects have already been established and where, after an objective examination of all of the relevant circumstances, such offences or acts having adverse effects may reasonably be suspected.¹²³⁸

Article 8(5) is primarily concerned with the latter sentence, on prospective criminal acts, and rightly limits them to specific and actual threats. The problem is that not only does the Directive fail to mention a predictable period for private actors to keep data in their databases, but it also does not provide the tools for carriers to know when, and if, they should delete the information, or make it anonymous.

The expectation of a possible use “at other points in time”¹²³⁹ created by Article 8(5) is too vague and undermines the legal clarity that air carriers should be able to rely upon. It is a serious incongruence that makes the retention of data by these actors go well beyond that which is necessary to ensure fulfilment of the purposes of the system.

Carriers should only be forced to retain data for those purposes until flight closure, save for updates to data they receive after that moment. In those cases, they should convey the new

¹²³⁶ Joined cases C-511/18, C-512/18 and C-520/18, paragraph 138.

¹²³⁷ *Idem*, paragraph 160.

¹²³⁸ *Idem*, paragraph 161.

¹²³⁹ Article 8(5) of Directive (EU) 2016/681.

elements to the PIUs automatically. That would suffice to ensure that the interference with fundamental rights is justified, while fully serving the needs of criminal investigations. Yet, this is very different from what is foreseen in the Directive, which appears disproportionate, and it may represent a rather heavy burden on small carriers.

It is a burden more insidious than first meets the eye. Article 12(4) says that “Member States shall ensure that the PNR data are deleted permanently upon expiry of the period referred to in paragraph 1.”¹²⁴⁰ That paragraph refers to data retained “in a database at the PIU.”¹²⁴¹ As such, there is no explicit time limit in the Directive regarding the retention of data stored in the databases of air carriers. And, according to the argument above, they are not free to eliminate data before the end of the retention period applicable to the PIUs. If they do so, they risk being unable to transfer them “at other points in time.”¹²⁴²

Additionally, if passengers take new international flights, their PNR receipts are updated in the databases of the PIUs, but also in the databases of carriers. As carriers must keep data to serve the purpose of Article 8(5), in practice, the renewal of receipts will also happen in their databases. And, if this happens, the same chilling effects can stem from the retention of data by private actors. Passengers may legitimately worry that their personal data can be stored without deletion, or interruption, not only in public databases but also in private archives, with little, if any, depersonalization guarantees. This certainly heightens the feeling of constant surveillance.

This system is not only disproportionate. It is internally and externally incongruent. Forcing all air carriers operating international flights to retain passenger data indefinitely goes against the very logic stated in the Directive of trying not to interfere with their business.¹²⁴³ It also defeats time and purpose limitation safeguards. It is, in addition, unclear how these provisions will work alongside the obligations to protect data and individual privacy that are imposed on carriers as a result of legislation such as Directive (UE) 2016/680 or Regulation (EU) 2016/679.

7. Right to notification

This final substantive section tackles an issue that was not addressed by the CJEU directly within the scope of the proportionality test. It is about the right to individual notification, which appears to be the basis for the exercise of all other data rights and the key to making passengers

¹²⁴⁰ Article 12(4) of Directive (EU) 2016/681.

¹²⁴¹ Article 12(1) of Directive (EU) 2016/681.

¹²⁴² Article 8(5) of Directive (EU) 2016/681.

¹²⁴³ See, for instance, recital (8) and Article 8 of Directive (EU) 2016/681.

aware of PNR. They can only protect their rights if authorities notify them whenever their personal data are accessed.¹²⁴⁴ This is an imperative of transparency.¹²⁴⁵

Susanna Villani argues that the jurisprudence makes notification a crucial element to judge the adequacy and necessity of big data-based policies.¹²⁴⁶ Notification procedures go against the logic that currently seems to permeate the intra-EU PNR system. Yet, such notification procedures could serve to weaken its chilling effects, not least because passengers would be able to know when, how, and for what reasons their data are used.

This obligation is, indeed, absent from the text of the Directive.¹²⁴⁷ Its provisions fail to reach the ambition expressed in recital (29), where the legislator wrote that:

Taking into account the right of passengers to be informed of the processing of their personal data, Member States should ensure that passengers are provided with accurate information that is easily accessible and easy to understand about the collection of PNR data, their transfer to the PIU and their rights as data subjects.¹²⁴⁸

Under the reference of Article 13(3), passengers benefit from a right to general information. However, the GDPR only says that they must be informed “when personal data are obtained.”¹²⁴⁹ This means that carriers must inform air passengers when they collect their data and transfer them to the PIUs.

Beyond that, notification is only foreseen in exceptional cases, when “a personal data breach is likely to result in a high risk for the protection of the personal data or affect the privacy of the data subject adversely.”¹²⁵⁰ In those circumstances, member states must “communicate that breach to the data subject and to the national supervisory authority without undue delay.”¹²⁵¹ This is a minimum guarantee that does not meet the standard required by the Court.

Such a standard would actually not be difficult to implement. It would make the system more balanced, even if it might seem to handicap the efficiency of police operations. Authorities would have to inform air passengers when processing their data,¹²⁵² except in automatic security

¹²⁴⁴ Opinion 1/15, paragraph 222.

¹²⁴⁵ *Idem*, paragraph 223.

¹²⁴⁶ Villani, 2018: 926.

¹²⁴⁷ Notification is different from the right to access to documents. Recital (30) stresses that the Directive does not hamper “the principle of public access to official documents.” Article 13(1) indeed foresees a right to this type of access, which suffices to comply with this requirement.

¹²⁴⁸ Recital (29) of Directive (EU) 2016/681. This idea is reinforced in recital (37). It partially repeats recital (29), saying that member states must “ensure that passengers are clearly and precisely informed about the collection of PNR data and their rights.”

¹²⁴⁹ Article 13(1) of Regulation (EU) 2016/679.

¹²⁵⁰ Article 13(8) of Directive (EU) 2016/681.

¹²⁵¹ *Idem*.

¹²⁵² Opinion 1/15, paragraph 223.

checks and organizational tasks handling aggregated files. These exceptions are easy to comprehend. Passengers are at any rate aware that their data are being analyzed in security checks. They consent to it, provided that carriers supply them with information adequately explaining the journey of their PNR data and that they are able to exercise their rights. On the other hand, it does not appear necessary to have air passengers notified when their information is being handled for organizational, or administrative, purposes alone. If data are aggregated and masked out, or if there is no access to the content of PNR receipts, there are no substantive reasons justifying notification. Beyond this, notification should also not be required whenever passengers may represent a concrete risk to the carrying out of criminal investigations.¹²⁵³

8. Closing remarks

In light of this analysis, it can be argued that the PNR Directive is not proportionate and should be declared invalid if a reference for a preliminary ruling were made to the Court. PNR interferes to a serious extent with the right to privacy laid out in Article 7 CFREU, by allowing large quantities of the personal data of identifiable passengers to be accessed by public actors for security purposes, and to be kept in huge databases on a continuous and systematic basis. It also seriously interferes with the right to data protection foreseen in Article 8 CFREU, as all data retrieved by the system are processed by automatic means.

On top of that, the intrusion on passengers' privacy reaches the point of interfering with the very essence of this right. The EU legislator should have considered alternative solutions to limit such interferences to that which is necessary to attain the public security purposes that the PNR system pursues. There are many aspects that need revisiting. Data should be retained on the basis of their relevance for public security, for instance, and the records of passengers with no criminal connections should be deleted as soon as PIUs first process them. Additionally, this piece of legislation should not allow for the collection of imprecise data, especially because it risks transferring sensitive material, the processing of which is prohibited. PNR does not ensure that all categories of sensitive data foreseen in Article 21 CFREU are excluded from processing.

Data are retained for an excessively long period of time. This analysis has tried to show why the CJEU should rethink its approach to this issue, and should start discussing the implications of the principle of necessity based on the genuine needs of law enforcement. Until this is done, passengers will continue to have their data held for unknown reasons in unknown archives for

¹²⁵³ Opinion 1/15, paragraph 224. See also joined cases C-511/18, C-512/18 and C-520/18, paragraph 191.

a very long time, potentially their entire lives. This causes chilling effects arising from constant surveillance. Besides, there are openings in the system that can allow data to be used for reasons and by entities beyond those expressly foreseen in the Directive. The depersonalization tools have serious gaps, with the result that not all data are masked out, and access to them is not dependent on prior review during the first six months after collection. Furthermore, data are not entirely protected when they are handled by private actors, since they may allow economic considerations to influence their decisions in the application of data protection guarantees.

These are some of the key takeaways to consider after this long and thorough study. Put together with the unsatisfactory notification scheme, it becomes clear why the intra-EU PNR system is not limited to that which is strictly necessary to fight serious crime and terrorism. It is an intrusive policy, working behind a veil of secrecy, which needs to be reconsidered. The bright side is that the EU legislator has the tools to draft a valid and proportionate PNR. It just needs to pay attention to the jurisprudence of the CJEU and the contributions of scholars and relevant auxiliary bodies.

Conclusions

“So far, there are little data about the added value of the PNR technology, although most law enforcement officials seem to be very confident about its success. What happens when one is put on a no-fly list by accident?”¹²⁵⁴

1. Main findings

This project has shed light on the validity of Directive (EU) 2016/681. It has sustained that the intra-EU PNR is unlawful for two main reasons. First, the Union legislated beyond its conferred powers by not respecting the security exception foreseen in treaty law that allows member states to regulate in relation to matters pertaining to their national security. Second, PNR violates the fundamental rights to privacy and data protection enshrined in the CFREU.

Chapter 1 tabled a comprehensive timeline of PNR in Europe. It filled a gap in scholarly writing since there are very few of such accounts, and none which are so detailed and up-to-date. This chapter began by looking at the AFSJ and how it is changing with the approval of policies which are premised on the need to deliver security at the expenses of individual privacy and the confidentiality of big troves of personal data. This is the context in which PNR was born. It is an instrument of pre-emptive justice fueled by big data collected by private actors through modern booking systems. Chapter 1 also introduced these systems, as well as API, the security scheme that preceded PNR. It then laid down the most relevant working definitions of concepts that are used in this research.

This was a document-based story, starting with the external agreements the Union celebrated with Australia, Canada, and the US. PNR was imported from alien legal systems and these agreements unveil some of the problems that it introduced into the EU’s legal edifice. PNR is a policy which results from compromise, and this is also palpable in the ongoing negotiations for future agreements with other third countries, as well as the multilateral strategy that the Union has been preparing to tackle transnational data transfers in a uniform way.

The development of an internal, EU-wide, PNR system occupied the last section of this chapter. The first discussions occurred in October 2003 but it was not approved until April 2016. It took 13 years to travel along this long and winding road. Still, some issues have managed to resist the test of time. Chapters 2 and 3 highlighted two such critical issues and tabled arguments to challenge the validity of the PNR Directive, claiming it should be annulled

¹²⁵⁴ Hert & Bellanova, 2011: 495.

by the CJEU. Chapter 2 explored the Union's lack of competence to approve such a PNR scheme and chapter 3 reflected upon this Directive's non-compliance with fundamental rights.

Chapter 2 presents an original argument in scholarly writing as PNR had never been properly analyzed from this angle. The first part of the chapter reviewed the legal bases of the Directive in the treaties. It argued that the EP and the Council of the EU went beyond the conferred powers laid out in Article 87(2)(a) TFEU by enacting a Directive providing for the retention of all booking data of all air passengers, in respect of all extra-EU flights, by law enforcement, instead of only data that may be regarded as strictly relevant to achieving its objectives.

The second part of the chapter extended the argument even further. It asserted that the Union did not have sufficient conferred powers to legislate so extensively on security because the member states retain some of their original powers, especially in relation to laws that may affect their national security agendas. While competences are shared in the AFSJ, according to Article 4(2)(j) TFEU, there are treaty law provisions designed to curb the logic of the principle of conferral to prevent the EU from freely adopting binding legal acts that might encroach excessively upon national security. This tension in primary law comes from the Treaty of Maastricht. The two provisions that appear to apply to the PNR case, and to restrict the EU's competence in this respect, are Articles 72 TFEU and 4(2) TEU, *in fine*.

Article 72 TFEU is characterized by structural and contextual problems that the Court has exploited over the years to weaken it. This security exception is nowadays void of almost all of its useful content, providing little leeway for member states to freely decide on the maintenance of law and order and the safeguarding of internal security. On the contrary, the CJEU has only recently started to explore Article 4 TEU. Despite the interpretative difficulties to which it gives rise, the Court's relative silence over the years and its seminal 2020 case law have created an opening that permits the possibility that, on a case-by-case basis, certain areas of national security remain the responsibility of member states. This provision is rather unique in the lexicon of conferral, which has made it more politically than legally relevant. Yet, the careful analysis included in this chapter permits us to salvage its normative content and see and exploit its potential in a way the literature had not done so far. By finding a middle ground between political wishful thinking and literal interpretation, it was possible to extract its core meaning and thereby challenge the EU's creeping competences.

The first step was to clarify its scope. Article 4(2) TEU, *in fine*, refers to the fight against very serious crime and terrorism, as well as intelligence actions and operations relating to state security. Secondly, the scope of sole responsibility was circumscribed in accordance with the logic of shared competences. This allowed for a revisiting of the Directive in order to ascertain

where the Union should have abstained from legislating in favor of residual competence for member states. On the one hand, PNR should be voluntary. On the other, certain norms should be reviewed and, in some cases, purged from the Directive. Article 4 should not address the organization of the PIUs, Article 6 did not need to define the detail of processing operations, Article 9 should be silent on the means used by competent authorities to cooperate, and Article 14 should not dwell on the sanctions that member states apply for non-compliance.

Chapter 3 was about fundamental rights. It was divided into three interdependent chapters that gradually helped to build the claim that PNR violates the CFREU. Scholars have presented many arguments against this legislative instrument in the last two decades. Still, most only scratch the surface of the problems they identify and few have written about the final version of the PNR Directive. This chapter has sought to fill this gap.

This was an immense task. To produce chapter 3 required reviewing countless pages of scholarly writing, contributions from the member states, parliamentary discussions, supervisory reports, and case law. A complete list of accessed documents would dwarf the annex of references and bibliography. Yet, this was imperative to properly dismiss weak and vague inferences and to develop promising lines of inquiry that could lead to robust arguments to substantiate the claim that PNR interferes with the fundamental rights of air passengers in a disproportionate manner. It was also necessary to show in detail the doctrinal steps that were taken to arrive at this conclusion.

Chapter 3.1 started by reviewing the literature. The arguments underpinning the doctrinal claims put forward at the end of the chapter can be glimpsed in preexisting works. Hitherto, however, many of the arguments presented are unripe. This chapter adds value by exploring and synthesizing the literature, which was yet to be done, and by making the authors figuratively enter into dialogue with one another, thereby shedding light on the flaws in their reasoning. The overarching topics that appear to frame the substantive discussions were the tension between security, privacy, and data protection; the fact of negative discrimination against certain categories of air travelers; and transparency in the exercise of individual data rights.

PNR has led to heated debates over the years. Many commentators acknowledge its risks and defects but end up charmed by the results and degree of control it can provide. And this is not exclusive to scholarly writing. The legislative process leading to its approval was also notable in this regard. No authors had previously discussed thoroughly the contributions of MEPs and national parliaments to the adoption of PNR and the relationship between PNR and fundamental rights. Chapter 3.1 took this step and placed their observations and interventions

side-by-side with the opinions of auxiliary and supervisory bodies to provide an unprecedented view-point in the literature.

The following chapter, chapter 3.2, provided a bridge between its neighbors. It was designed to prepare the reader for the structure of the doctrinal claims that are presented in chapter 3.3. Chapter 3.2 assessed two recent decisions of the CJEU, joined cases C-293/12 and C-594/12 and Opinion 1/15. The Court declared that Directive 2006/24/EC and the 2014 EU-Canada Agreement were incompatible with Articles 7 and 8 CFREU.

The formal structure of this chapter mimicked the one used by the Court in these judgments, and that which is commonly found in the case law applying proportionality tests to security legislation. This is an authoritative method, derived as it is from the actual approach of the CJEU, and was, consequently, chosen to give consistency and clarity to the presentation of the doctrinal claims. Each ruling was dissected in chapter 3.2 in accordance with the Court's approach. Nonetheless, the judicial reasoning was not entirely summarized since this was a targeted analysis, the purpose of which was to conclude the search for arguments relevant for a legal evaluation of the intra-EU PNR. This purpose steered the choice of Court decisions to analyze, as well as of the legal arguments to highlight.

Chapter 3.3 is shaped almost as a preliminary ruling from the CJEU would be, adopting the same structure as in the preceding chapter. It began by revealing how PNR seriously interferes with the privacy and data protection rights of passengers. These rights were initially examined separately, in line with an increasing trend in scholarly literature that sees data protection as a sufficiently mature right deserving independence from privacy. Reasons of space and time, together with a need for conciseness, however, forced the use of a single proportionality test.

The chapter claimed that the Directive is unlawful because of the quantity and quality of data collected for law enforcement purposes, the length of the retention period, and the manner in which third parties can access PNR data. While it may be adequate to attain the objectives it pursues, it is not limited to that which is strictly necessary. It allows for the indiscriminate retention by law enforcement of all the personal data included in the PNR receipts of passengers of international flights, while not fully barring the processing of sensitive elements. Secondly, the information is held for a very long time without there being different retention periods depending on the investigatory relevance of data and air passengers. The system also does not guarantee the irreversible destruction of the data collected at the end of the retention period. What is more, unknown authorities may use PNR for purposes beyond those expressly foreseen in the Directive, PNR receipts are not anonymized immediately after collection, non-independent and non-judicial authorities can authorize access to data, and the information can

be transferred to third countries that do not guarantee an adequate level of data protection. Besides, air carriers are allowed to take into consideration economic factors when choosing how they will protect data.

At the time of writing, there were already pending cases before the Court which query the validity of PNR. At least six applications and requests for preliminary rulings were based on issues addressed in chapter 3, with privacy and data protection taking the front seat. While some were tabled by member states, others were lodged by carriers or other private actors like human rights organizations. Any judgement laid down by the CJEU will have an important impact on the aviation sector, both within and outside the Union. It seems quite likely that the Directive will be regarded as invalid. Nonetheless, the added value of this project will remain in any case, not only due to the comprehensive doctrinal analysis which it presents, but also due to the originality of the research.

PNR is a novel security measure in the context of EU law. It was born in an atmosphere of fear, but also of technological sophistication. These factors combined can raise serious hurdles for the protection of fundamental rights and for the legal principles that guide the Union as a matter of law. New counter-terrorism policies, like PNR, will continue to be adopted at member state and EU-level. However, this study has sought to buttress the idea that the ends do not (always) justify the means. Despite the arguments presented in this thesis, it is acknowledged that PNR can and should become an important tool to tie up the loose ends in data monitoring left by existing pre-emptive security policies. Therefore, this work has firmly rejected the idea that an intra-EU scheme is not necessary. It can actually be crucial to achieve the goals of the AFSJ, and even purposes well beyond the security agenda. The thesis accepts that as:

Member States have...pointed out [using] PNR data could constitute a valuable tool to protect public health and prevent the spread of infectious diseases, for example by facilitating contact tracing as regards persons who have been sitting near an infected passenger. This issue has gained even more prominence since the emergence of the COVID-19 pandemic.¹²⁵⁵

Nonetheless, PNR has a long way to travel to strike the right balance between security, privacy, data protection, and individual data rights. This will require a substantial effort involving institutional cooperation between the Union and the member states regarding security strategies. And while these strategies must be effective and efficient, policymakers should resist

¹²⁵⁵ Report (COM(2020) 305 final, 24.7.2020), 11.

taking shortcuts when providing for the processing of big data. Fundamental rights and the rule of law must always steer how PNR and, indeed, all kinds of personal data are to be handled.

2. Broader lessons

The previous section has conveyed the key takeaways of this thesis. The story of PNR in Europe, however, has a lot more to tell us about the EU and the way it is evolving. In the course of this research, topics have arisen that need further discussion and closer engagement by both scholars and institutional actors. There are broader lessons to learn for the future of the Union and EU law beyond those pertaining to the validity of Directive (EU) 2016/681, or the balance of security competences in the AFSJ. These last pages do not explore these broader lessons in depth but lay out some key ideas that merit further reflection, thereby setting an agenda for future research in this area. This section talks about the implications of PNR for the future of fundamental rights, the effects of terrorism on regulatory change, the position of the EU as global actor standing for the protection of personal data and fundamental rights, and the lack of adequate impact assessments supporting PNR.

2.1 A poisoned package

While the GDPR has been hailed as the “most consequential regulatory development in information policy in a generation,”¹²⁵⁶ PNR has been found “to be so risky for the protection of fundamental rights that careful scrutiny needs to be made to the relevant regulatory text.”¹²⁵⁷ These legal acts are part of a composite regulatory effort and were approved on the same day. However, they follow different directions and actually serve clashing purposes. The legislative package of April 2016 has both strengthened and weakened the protection of personal data and other fundamental rights of EU consumers.

It is not entirely clear where the trade-off between security and human rights stands in relation to a package deal such as this one. The Union has presented its citizens with what can be seen as a poisoned package. While it took a rather defensive approach through the adoption of the GDPR, as regards the processing of online data, it nevertheless accepted that, in certain circumstances, much of that same data can be collected and made widely available, subject to considerable fewer guarantees, in order to monitor what individuals are up to. With the right

¹²⁵⁶ Hoofnagle, et al., 2019: 66.

¹²⁵⁷ Chiappetta & Battaglia, 2018: 78.

trigger, traditional criminal procedure law can be ‘adapted’ to make sure that the police and other law enforcement entities have broad access to large quantities of personal data with a view to fighting crime.

The future of fundamental rights such as privacy and data protection, as well as the use of pervasive technology to combat prospective threats, are matters that will remain at the center of the European political arena for a long time. These issues will always be controversial and continue to stimulate an ever-growing debate. PNR exemplifies the nature of these discussions and debates. Opinions are divided regarding almost all of its features. And it is worrying that the EU is emulating countries like the US in adopting security policies that provide few or no alternatives to people when personal data are to be exposed and which are not accompanied by sufficient guarantees that privacy and the presumption of innocence will be respected.

The CJEU has played a critical role in the journey of PNR and in relation to the broader interplay of security and fundamental rights. It has been perceived as a champion of data protection in its recent jurisprudence but it has also prevented member states from enjoying significant leeway when deciding on their national and internal security policies. It has deprived security exceptions foreseen in the treaties of bite and has thereby expanded EU competences in a way that causes friction in the cooperation logic permeating the AFSJ. Considering that security is a sensitive matter closely linked to statehood and sovereignty, the Court’s resistance to using interpretative tools that result in deference to national legislators in areas of national security may, in the end, weaken integration and endanger the idea of unity in diversity.

It is thus for the CJEU to reflect on the meaning and limits of its rulings. The intersection of discussions on competence and concrete security policies might help steer its reading of security exceptions, giving power to the member states and trusting that they can protect fundamental rights in a balanced manner.

2.2 Demonstration effects

Chapter 1 took us into the journey of PNR in the EU. Zooming in on the year before its approval reveals a timeline where terrorist events were the trigger for significant regulatory change. The fear-based haste to enact policies that aim to counter complex crime and terrorism, and the goal of mitigating public fears, might begin to explain why the EU legislator passed an internal PNR system that interferes so aggressively with the private lives of air passengers and leaves their personal data insufficiently protected.

After the draft proposal of 2011 was rejected on 24 April 2013, the project of an intra-EU PNR was sidelined by the LIBE Committee. Yet, on 7 January 2015, a terrorist attack against the newspaper Charlie Hebdo, in Paris, killed a dozen people.¹²⁵⁸ A similar event occurred by the end of the year. On 13 November, “gunmen and suicide bombers hit a concert hall, a major stadium, restaurants and bars, almost simultaneously - and left 130 people dead and hundreds wounded.”¹²⁵⁹ And, on 22 March 2016, there were bombings in the main terminal of Zaventem airport and in a metro station, in Brussels, killing 32 people and injuring many more.¹²⁶⁰

Scholars have tried to demonstrate that such incidents were the turning point that brought PNR back on the EU’s policy agenda and were linked to the fast-tracking of the Directive. Estelle Massé and Lucie Krahulcova wrote in the blog of the human rights organization Access Now that its approval was “no more than a knee-jerk reaction to the political climate after the terrorist attacks in Paris and Brussels.”¹²⁶¹ They have also argued that the awareness raised by advisory bodies about the deficiencies of PNR regarding fundamental rights did not produce the expected outcome probably because this climate of fear diverted the attention of policymakers from fundamental rights to the security agenda.

In fact, on 11 February 2015, about a month after the first attack in Paris, the EP issued a Resolution showing its commitment to draft a Directive on PNR that year.¹²⁶² Its recitals reveal that this was a direct institutional response to that incident. The EP was worried that, ever since 9/11, terrorism was negatively impacting the public’s perception of security,¹²⁶³ especially in face of the rising danger of foreign terrorist fighters.¹²⁶⁴ Following the second attack on the French capital, on 25 November, the EP issued a new Resolution reiterating the aim of having a EU PNR ready in 2015. This was one of a set of measures to step up the response to radicalization in Europe, undertaken together in an ambitious approach to fight terrorism and crime.¹²⁶⁵ This Resolution also mentioned that it had been issued in the aftermath of the Paris incidents.¹²⁶⁶ The EP would later acknowledge that the “November Paris attacks gave impetus to a compromise [on PNR], subsequently endorsed by the Council and backed by LIBE in December 2015.”¹²⁶⁷

¹²⁵⁸ BBC, 2015 (a).

¹²⁵⁹ BBC, 2015 (b).

¹²⁶⁰ BBC, 2016.

¹²⁶¹ Massé & Krahulcova, 2016.

¹²⁶² European Parliament Resolution (OJ C 310, 25.8.2016), paragraph 13.

¹²⁶³ *Idem*, recital (E).

¹²⁶⁴ *Idem*, recital (G).

¹²⁶⁵ European Parliament Resolution (OJ C 366, 27.10.2017), paragraph 42.

¹²⁶⁶ *Idem*, recitals (C) and (D). See also paragraph 1.

¹²⁶⁷ European Parliamentary Research Service, 2016.

In 2013, the LIBE Committee rejected the 2011 proposal by 30 votes to 25. By the end of 2015, it backed the new draft with 38 votes to 19. PNR was never a consensual matter but it was still approved, despite its inherent problems. Its return was the result of social and political pressure for some sort of change at the regulatory level, even if both that pressure and the resulting legislation were far from hitting the (right) target.

PNR is a painful example of the theory of demonstration effects, formulated by scholars like Walter Mattli or Ngaire Woods. They have written that the “emergence of broad societal demand for change is a function of the diffusion of information about the social cost of the regulatory status quo via glaring inadequacies and failures (demonstration effects).”¹²⁶⁸ The immediate public and media outcry after the Paris and Brussels attacks¹²⁶⁹ led EU and national legislative institutions to believe there was a gap in aviation data security systems that could be explored by foreign terrorist fighters and other criminals to commit serious crimes and acts of terror, despite the already tight security coating applicable to air transportation.

There was a sort of misdirected consensus that the *status quo* on aviation security was flawed and that the cost of ‘upgrading’ it would be justified and proportionate. It seemed that more and broader security and regulatory tools were needed to ensure that no data escaped monitoring by law enforcement. So, instead of less and targeted data retention operations, the option taken at the time was to guarantee that all booking information was collected, analyzed, and used to anticipate and deter any prospective acts of terror. PNR, with its seeming capacity to identify “persons who were unsuspected of involvement in terrorist offences or serious crime prior to...an assessment [of their] PNR data,”¹²⁷⁰ appeared as the silver bullet, the policy solution that could stop offenders from exploiting civil aviation for criminal purposes and restore peace and security. Plus, it had the benefit of not being an unheard-of policy since it had been on the Union’s agenda before and it was part and parcel of the normal business of air carriers.

The problem, however, is the hidden social cost of PNR, i.e., its heavy burden on fundamental rights. MEPs approved legislation in the aftermath of criminal events which had a large impact in social media and on public opinion, which merely focused on the end-result without noticing competence concerns or gaps in the protection of fundamental rights. The superficial debate in the legislative process and the flaws of the legislation are sufficient to claim that the whole PNR journey has shortcomings that should make the Union and the member states reflect on their desire for mass data collection and their preferred mode for

¹²⁶⁸ Mattli & Woods, 2009: 24.

¹²⁶⁹ Bigo, et al., 2016.

¹²⁷⁰ Recital (7) of Directive (EU) 2016/681.

tackling serious crime and terrorism. The fact that they did not discuss the full risks of profiling or the risks of endorsing so lengthy a data retention period are just two of the most striking gaps in the deliberations of MEPs. And they had the tools at their disposal to deliberate in depth, not least due to the rich jurisprudence of the CJEU, scholarly writing, and, perhaps above all, the relevant collection of reports and documents issued by supervisory bodies.

The role of these supervisory bodies, especially the EDPS, in raising awareness over the years of the limitations of the intra-EU PNR should make MEPs seriously reassess the piece of legislation that they approved and the way in which the EP conducts debates on security. Searching for ‘PNR’ in the EDPS’s online database turns out 158 publications issued by this supervisor alone.¹²⁷¹ It is striking that many of the concerns it tabled before the EP were largely ignored. The reports of this body contain a repository of most issues affecting PNR. They convey, and often anticipate, much of the criticism put forward by scholars and the Court. Still, the EDPS was not mentioned in the PNR legislative debate, as was the case with other supervisory and regulatory bodies. They could, perhaps, have been called to participate in a more direct fashion. Their role in the legislative process could have been strengthened not only by having MEPs pay more attention to their opinions but also by summoning representatives of these bodies to present their views orally in the debates.

Their participation could have softened the fear and lessened the haste to approve this new security measure, likewise appeasing public opinion. Having supervisory bodies contribute more conspicuously in these processes could help shed light on the social and fundamental rights’ costs of regulating security. Those who militated for change in the aftermath of the Paris and Brussels terrorist events would have been better served by a system that was responsive to the comments and suggestions made by the EDPS. Supervisors enjoy important insights into what must change, what should remain unchanged, and how to secure appropriate change.

An example of how supervisory bodies could have helped to strike a more appropriate balance between fundamental rights and security can be seen in the references of MEPs to the GDPR. Some argued that the entry into force of PNR at the same time as the data protection package helped to secure the right balance between fundamental rights and security; that the flaws of the PNR Directive were somehow mitigated by the timing of its approval. However, they have failed to explain why they consider this to be the case. It seems this is little more than a false perception. PNR and the GDPR are different regimes and this thesis has demonstrated that the references of the Directive to the GDPR are not sufficient to protect the rights of air

¹²⁷¹ European Data Protection Supervisor, 2021.

passengers. Backed by their own independent research, the EDPS and other supervisors would certainly have been able to explain this misconception to the MEPs.

2.3 Contingent unilateralism and hypocrisy

The quote at the beginning of chapter 3.3 is about what distinguishes a hypocrite from the rest of us. In short, a hypocrite is someone who has endorsed a mismatch between their actions and pronouncements in a way that undermines his or her “claim to moral authority.”¹²⁷² The intention behind this quote was to criticize how the EU dealt with PNR. It was announced as a security policy that would respect fundamental rights and keep citizens safe¹²⁷³ but it blatantly tramples over fundamental rights, was approved with little care for the privacy of innocent passengers, and its efficiency is highly questionable, as will be shown below. The Union was hypocritical throughout the journey leading to the adoption of the intra-EU PNR and its claim to moral authority concerning fundamental rights is clearly undermined as a result of the approval of this aggressive policy of big data retention and broad-scale monitoring.

Reasons of space have forced the removal of explanatory comments to this quote from that chapter. Yet, the arguments made there give flesh to the idea that the EU is faltering as a bastion of human and fundamental rights when faced with the appeal of modern technologies to help fight crime through the collection of personal data. This is why such quote was left to introduce the legal analysis.

The claim to moral authority can also be found by reading between the lines of the references in chapter 1 to the PNR agreements with third countries. Such agreements serve to protect PNR data that are transferred to outside the Union. But that is not the whole story. In fact, the EU concluded these agreements to satisfy the demands of relevant economic partners that were pressuring air carriers into sending them all the booking data of EU passengers flying to, from, or through their territories. Australia, Canada, and the US have undoubtedly won the iron fist after threatening the Union that carriers would lose landing rights if it did not comply. Yet, despite their continual review and the usual assertiveness of the EU in exporting its values, there are no reciprocity clauses in the PNR agreements. Carriers must send data to the security and border agencies of those third countries but not to EU entities, or their equivalent in the member states. Such clauses could, notwithstanding, be a valuable instrument for the Union to

¹²⁷² Isserow & Klein, 2017: 193.

¹²⁷³ See, for instance, recitals (15), (20), (22), (28), (29), and (36), as well as Articles 13 and 15 of Directive (EU) 2016/681.

ensure that third countries maintain high data protection standards when processing data. They are relevant as a tool to protect individual data but also as a trump card in dialogs.

The EU has also announced ongoing negotiations with other third countries and a common, multilateral, PNR scheme to harmonize transfers and guarantee the same level of data protection across the board. Such a common instrument could prove to be a crucial step in light of the growing use of PNR systems by countries with very different attitudes to human rights compared to the EU. However, neither these new agreements nor the harmonized template are a reality nowadays.

It has been more than a decade since the Commission published a Communication tabling its “global approach towards PNR transfers to third countries [foreseeing] a number of data protection principles and safeguards.”¹²⁷⁴ Its website on these matters reveals a gap between 2010, when that approach was first introduced, and 2020, when the Commission issued a roadmap aiming at “setting out the policy objectives and key challenges of both legal and operational nature [for] a future revised strategy.”¹²⁷⁵ This is an acknowledgment that the Commission has done very little, if anything, of relevance regarding the protection of the personal data of air passengers outside Union borders.

So, while the EU has announced that it cares for the privacy and data protection of its citizens by pushing for a multilateral arrangement and by including certain provisions to protect data in the PNR agreements, it has, in practice, been a rather hypocritical player in this game. On the one hand, Opinion 1/15 of the CJEU clearly shows that the data protection mechanisms included in the Agreement with Canada are far from adequate. On the other, there have been no substantial developments towards a common approach to keep PNR data safe when transferred overseas in more than a decade.

Is the Commission afraid to upset economic interests by raising the bar in terms of fundamental rights’ protection or even by imposing a single, robust, multilateral template when negotiating PNR agreements? Or does it consider that failing to ensure the safety and security of the personal data of EU air passengers is justified when balanced against the profit and stability that stem from obeying the demands of its economic partners?

The position of the Union as a global actor in terms of data protection and fundamental rights more broadly is not very favorable from this angle. We could perhaps have hoped to witness an example of contingent unilateralism. This expression is used by scholars to describe the use of unilateral EU instruments to serve as a catalyst to export EU values outside the Union in

¹²⁷⁴ European Commission, 2021.

¹²⁷⁵ *Ibidem*.

circumstances where otherwise there is a lack of political will on the part of third countries to go in the same direction.¹²⁷⁶ In this case, the internal EU-PNR, and limitations on data export included therein, could have been used to encourage third countries to improve the level of data protection included in bilateral PNR agreements. Alas, in the case of PNR, and by contrast with the GDPR,¹²⁷⁷ the European position was characterized by weak resolve externally and by a consequently diminished role for the EU as a contingent unilateralist.

The hypocritical side of the PNR story can be further explored if the PNR Directive does end up being invalidated by the CJEU. If this happens, in line with what is argued in this thesis, talking about promoting the protection of personal data at a global level becomes indefensible given that the Union has failed to protect data at home. Can the EU even contemplate being a normative global actor, holding and promoting firm positions regarding data protection and privacy laws externally, if its internal PNR system is found to be inadequate by the standards of its own primary law?

2.4 Effectiveness reports

In December 2019, the civil rights organizations Society for Civil Rights - Gesellschaft für Freiheitsrechte e.V. (GFF) and epicenter.works - Plattform Grundrechtspolitik held a presentation as part of their campaign #NoPNR. Let's kill the next Data Retention Law. One of the most striking matters they talked about was the effectiveness rates of EU PNR systems in achieving their purposes and in successfully targeting suspicious passengers.

According to the presenters, from the transposition of the PNR Directive in 2018 until mid-August 2019, the PIU operating in Germany checked 31 617 068 PNR receipts. There were 237 643 positive matches, from which 910 were relevant for criminal investigations. The numbers of false positives and true hits are unknown but 910 hits correspond to about 0.4% of positive matches and only 0.003% of all PNR receipts verified. 57 people were consequently detained or arrested, which corresponds roughly to 0.0002% of screened passengers. It is not known for what crimes they were targeted.

The numbers for Austria were also presented. Until 30 September 2019, 23 877 277 PNR receipts of about 11 900 000 travelers were verified. There were 190 541 positive matches, from which only 280 were deemed relevant for law enforcement operations. The numbers of false positives, true hits, arrests, or detentions were not disclosed. 280 hits correspond to about

¹²⁷⁶ Scott & Rajamani, 2013: 209.

¹²⁷⁷ Kuner, 2019: 132.

0.15% of positive matches and 0.001% of checked receipts. In the meanwhile, the Austrian PIU costs about 1 840 570 € per year to maintain.

The gap between processed PNR receipts and useful hits was known to EU institutions before the approval of Directive (EU) 2016/681. As was mentioned in chapter 3.2, in Opinion 1/15, the CJEU said that the Commission had “noted in its written observations that, according to the information provided by the CBSA, the processing of PNR data ha[d]...enabled the arrest of 178 persons from among the 28 million travellers who flew between the European Union and Canada in the period from April 2014 to March 2015.”¹²⁷⁸ PNR data had also led to “drugs seizures in 71 cases and seizures of child pornography material in two cases. That data also made it possible to initiate or further pursue investigations in relation to terrorism in 169 cases.”¹²⁷⁹ Even if these cases are considered separately and discarding false positives, it means that, out of 28 million people who had their personal data collected, only 420 cases represented positive matches. 420 matches correspond to about 0.0015% of the receipts verified.

These numbers are shocking. The claim to moral authority discussed above again quickly springs to mind as a result of these figures. The EU approved a pervasive system that allows for the collection and processing of millions of entries of personal data and which violates the fundamental rights of European citizens and aliens alike on a systemic and systematic basis to deliver an output that is insignificant, marginal at best. It did so without presenting a single report, study, or impact assessment on the capacity of PNR to effectively attain its goals.

There are many questions that can be asked in face of the marginal percentage of actual hits. One wonders whether a study conducted in advance of the issuing of the legislative proposal for PNR, or even in the course of the legislative process, would not have prevented the legislator from enacting PNR. The last attempted terrorist attack in the airside of an EU airport or in aircrafts dates back to 2009. On 25 December, Umar Abdulmutallab, a 23-years-old Nigerian man tried to detonate explosives concealed in his underwear on a flight from Amsterdam to Detroit. Considering the low number of positive hits and the significant security mechanisms that already apply to air transportation, from the general ban on liquids to massive screening, it is natural to wonder whether the processing of API and all the other monitoring tools are not sufficient to deliver the same results in the fight against crime and terrorism. PNR appears to be very far from delivering upon the promised deterrence and unprecedented effectiveness that its supporters claimed. Yet, its social and fundamental rights’ cost is far heavier than that of those other security tools.

¹²⁷⁸ Opinion 1/15, paragraph 152.

¹²⁷⁹ *Idem*, paragraph 56.

Did the EU consciously skip drafting an impact assessment on effectiveness because it knew PNR was not an efficient tool? This is a terrifying question. It was certainly not for lack of warning since scholars and supervisory bodies have emphasized repeatedly over the years the importance of assessing its effectiveness. Chapter 3.1 revealed that the EDPS has pressed the EU legislator, at least since 2011, to provide impact assessments whenever “the substance of the Proposal affects the fundamental rights to privacy and data protection.”¹²⁸⁰ However, there were no assessments produced comparing the figures of prospective air passengers and positive matches. Its concerns were ignored, as were those of authors such as Maria Tzanou, who stressed that the reasons tabled by the Commission to implement an EU-wide PNR were “not very convincing as empirical evidence on PNR system effectiveness [was] lacking.”¹²⁸¹ Mathias Bug and Sebastian Bukow would reinforce this, saying that PNR, like the data retention Directive, affects “the entire society, independent of concrete evidence.”¹²⁸²

Enerstvedt has undertaken an ample study on aviation security and found that occasional reports, mainly from the United Kingdom and the US, have shown that PNR can, indeed, be instrumental in locating criminals and preventing terrorist attacks. Nonetheless, they often fail to mention how many passengers have to be investigated to arrive at positive results, or whether other security apparatuses would have been sufficient to achieve the same outcome. The real question, for now, is not so much whether a “100% success rate is...realistic [but rather] whether profiling and the failure rates are acceptable or not.”¹²⁸³ This is, undeniably, the most relevant discussion and it necessitates a previous step of compiling detailed statistics, figures, and updated information on the concrete effectiveness of PNR. Why these data were not compiled in the course of the legislative process is a question that needs to be urgently addressed.

Based on the work of the Article 29 Working Party, the Commission has only provided anecdotal evidence about the effectiveness of PNR. Whenever it has tried to justify its use, the Commission has showcased those occasions where such data were instrumental for the success of criminal searches, shunning the majority of cases where PNR data led to the targeting of innocent passengers. There are, to this day:

[N]o statistics showing the ratio between the number of innocent travellers whose PNR data [were] collected to the number of law enforcement outcomes resulting

¹²⁸⁰ Opinion of the EDPS (OJ C 181, 22.6.2011), paragraph 25.

¹²⁸¹ Tzanou, 2015: 97.

¹²⁸² Bug & Bukow, 2017: 292.

¹²⁸³ Enerstvedt, 2017: 276.

from that PNR data. Although some terrorist attacks could have been avoided, if a PNR scheme had already been in place, no evidence or facts were given.¹²⁸⁴

This is true for the intra-EU PNR but also for the agreements with third countries. Even “[r]eports of the US Government Accountability Office [have] not confirm[ed] the efficiency of PNR.”¹²⁸⁵ Effectiveness reports could generate to an informed discussion on the value of this system and of alternative available tools for law enforcement. David Lowe is wrong in stating bluntly that PNR has “contributed in making it difficult for terrorists to use aircraft in acts of terrorism.”¹²⁸⁶ This might be a reasonable first impression, or general feeling, but there is no evidence of that. The numbers shown above and the opacity of the system do not support this claim. And even those figures only concern certain countries. There is as yet no broad assessment on the effectiveness of PNR across the member states. Significantly, and worryingly, the 2020 review also failed to address this matter. The failure to conduct thorough and transparent impact assessments prior to the approval of legislation, or indeed in the course of later reviews, is an important epistemic shortcoming characterizing EU security law.

This problem is not exclusive to PNR. Since the turn of the century, the Union has expanded the AFSJ with the implementation of a series of security policies based on the retention of big data and the creation of diverse entities to manage both the processing and exchange of information across the member states. Scholars have pointed to the fact that, in the overall, “[v]ery little is known about the effectiveness, proportionality or added value of this EU counterterrorism architecture, its tools or actors.”¹²⁸⁷

One of the final slides presented by the speaker from Society for Civil Rights in the 2019 congress stated that the PNR Directive allows for a sort of “miracle weapon”¹²⁸⁸ in terms of data processing. This weapon is the automatic profiling undertaken by the PIUs, which allows for “hundreds of millions of people [to be] affected for simply using a plane [and] sets a dangerous precedent for mass surveillance.”¹²⁸⁹ Comparing the small numbers of useful hits to the massive numbers of people who are targeted and the huge quantities of data that are processed, makes it frightening to think that PNR might serve to lay the foundations of a digital surveillance state. It is to be hoped that the CJEU will step in where other institutions have

¹²⁸⁴ Enerstvedt, 2017: 275.

¹²⁸⁵ *Ibidem*.

¹²⁸⁶ Lowe, 2016: 879.

¹²⁸⁷ Bigo, et al., 2016.

¹²⁸⁸ Available at https://c3media.vsos.ethz.ch/congress/2019/h264-hd/36c3-10919-eng-deu-fra-NoPNR_-_Lets_kill_the_next_Data_Retention_Law_hd.mp4 (accessed on 25 February 2021).

¹²⁸⁹ *Idem*.

failed, thereby pushing the EU in the direction of ensuring that its security interests, and the security interests of its member states, can be effectively protected and appropriately balanced while ensuring respect for human rights.

Annex: References

A. Legislation and policy documents

1. Council of Europe

Convention for the protection of individuals with regard to automatic processing of personal data (European Treaty Series 108, 28.1.1981)

Recommendation of the Committee of Ministers to member states regulating the use of personal data in the police sector (R(87) 15, 17.9.1987)

Recommendation of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (CM/Rec(2010) 13, 23.11.2010)

2. EU

2.1 Primary law

Charter of Fundamental Rights of the European Union (OJ C 326, 26.10.2012)

Treaty on European Union (OJ C 191, 29.7.1992)

Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts (OJ C 340, 10.11.1997)

Treaty of Nice amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts (OJ C 80, 10.3.2001)

Treaty establishing a Constitution for Europe (OJ 2004/C 310, 16.12.2004)

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (OJ C 306, 17.12.2007)

2.2 Secondary law

2.2.1 Commission

Communication to the Council and the Parliament on the transfer of air Passenger Name Record (PNR) data: A global EU approach (COM(2003) 826 final, 16.12.2003)

Communication to the European Parliament and the Council ‘Overview of information management in the area of freedom, security and justice’ (COM(2010) 385 final, 20.7.2010)

Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries (COM(2010) 492 final, 21.9.2010)

Communication to the European Parliament, the European Council and the Council ‘First progress report towards an effective and genuine security Union’(COM(2016) 670 final,

12.10.2016)

Communication to the European Parliament and the Council ‘Exchanging and protecting personal data in a globalised world’ (COM(2017) 7 final, 10.1.2017)

Communication to the European Parliament, the European Council and the Council ‘Fifteenth progress report towards an effective and genuine security Union’ (COM(2018) 470 final, 13.6.2018)

Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (2002/2/EC) (OJ L 2, 4.1.2002)

Decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States’ Bureau of Customs and Border Protection (2004/535/EC) (OJ L 235, 6.7.2004)

Decision of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency (2006/253/EC) (OJ L 91, 29.3.2006)

Implementing Decision (EU) 2017/759 of 28 April 2017 on the common protocols and data formats to be used by air carriers when transferring PNR data to Passenger Information Units (OJ L 113, 29.4.2017)

Joint statement: Beginning of negotiations between Mexico and the European Union on PNR data transmission (STATEMENT/15/5374, 14.7.2015)

Regulation (EEC) 2672/88 of 26 July 1988 on the application of Article 85 (3) of the Treaty to certain categories of agreements between undertakings relating to computer reservation systems for air transport services (OJ L 239, 30.8.1988)

Report on the application of Council Regulation (EEC) 2299/89 of 24 July 1989 (COM(97) 246 final, 9.7.1997)

Report to the European Parliament and the Council on the joint review of the implementation of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service {SWD(2014) 236 final} (COM(2014) 458 final, 10.7.2014)

Report to the European Parliament and the Council on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security {SWD(2017) 14 final} {SWD(2017) 20 final} (COM(2017) 29 final, 19.1.2017)

Report to the European Parliament and the Council on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2020) 305 final, 24.7.2020)

Staff working document ‘Implementation plan for Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime’ (SWD(2016) 426 final, 28.11.2016)

Staff working document accompanying the ‘Report from the Commission to the European Parliament and the Council on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime {COM(2020) 305 final} (SWD(2020) 128 final, 24.7.2020)

Staff working paper ‘Impact Assessment’ (SEC(2011) 132 final, 2.2.2011)

2.2.2 Council

Decision of 12 February 2007 establishing for the period 2007 to 2013, as part of General Programme on security and safeguarding liberties, the Specific Programme ‘Prevention of and fight against crime’ (2007/125/JHA) (OJ L 58, 24.2.2007)

Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (OJ L 261, 6.8.2004)

Proposal for a Decision on the conclusion of an Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information (API)/Passenger Name Record (PNR) data (COM(2005) 200 final, 2005/0095 (CNS), 19.05.2005)

Proposal for a Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes {SEC(2007) 1422} {SEC(2007) 1453} (COM(2007) 654 final, 2007/0237 (CNS), 6.11.2007)

Regulation (EEC) 2299/89 of 24 July 1989 on a code of conduct for computerized reservation systems (OJ L 220, 29.7.1989)

Regulation (EC) 323/1999 of 8 February 1999 amending Regulation (EEC) 2299/89 on a code of conduct for computer reservation systems (CRSs) (OJ L 40, 13.2.1999)

2.2.3 Council of the EU

Decision authorising the opening of negotiations with Japan for an agreement between the European Union and Japan on the transfer and use of Passenger Name Record (PNR) data to prevent and combat terrorism and serious transnational crime (5378/20, 4.2.2020)

Decision of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program (OJ L 195, 27.7.2010)

Declaration condemning the terrorist attacks on London (11116/05 (Presse 187), C/05/187, 13.7.2005)

Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA) (OJ L 164, 22.6.2002)

Framework Decision of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (2008/977/JHA) (OJ L 350, 30.12.2008)

Information Note from the General Secretariat to the Permanent Representatives of the Committee and Council on the judgment of the Court of 8 April 2014 in joined cases C-293/12 and C-594/12 – Invalidation of 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 (9009/14, 5.5.2014)

Note from the General Secretariat ‘Declaration on combating terrorism’ (7906/04, 29.3.2004)

Note from the Presidency and CT Co-ordinator to the Council/European Council on the European Union counter-terrorism strategy (14469/4/05 REV 4, 30.11.2005)

Note from the Presidency to the Coreper/Council (10439/08, 10.6.2008)

Note from the Presidency to the Multidisciplinary group on organised crime (5618/2/09 REV 2, 29.6.2009)

Note from the Spanish delegation to the Council on the information by the Commission on the PNR legislation adopted by Mexico and the Republic of Argentina requesting the transfer of PNR data from the EU (6857/15, 5.3.2015)

Note on the voting result of Directive of the European Parliament and of the Council on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (First reading) (8267/16, 25.4.2016)

Note from the Presidency to the Working Party on Information Exchange and Data Protection (DAPIX) on the Conference on the future of PNR data - effective use and challenges (6104/18, 23.2.2018)

Note from the Presidency to the Permanent Representatives Committee/Council on the Directive (EU) 2016/681 on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime - Implementation of the PNR Directive / Exchange of views (6017/18, 26.2.2018)

Note from the General Secretariat to the Working Party on Information Exchange and Data Protection (DAPIX) on the Update on the Informal Working Group on PNR (10139/18, 21.6.2018)

Note from the General Secretariat to the Working Party on Information Exchange and Data Protection (DAPIX) on the update on the Informal Working Group on PNR^[1]_{SEP}- 7th IWG PNR meeting (12825/18, 17.10.2018)

Proposal for a Decision on the conclusion of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service (2011/0126 (NLE)) (COM(2011) 281 final, 19.5.2011)

Proposal for a Decision on the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data 2013/0251 (NLE) (COM(2013) 529 final, 18.7.2013)

Recommendation for a Decision authorising the opening of negotiations on an Agreement between the European Union and Canada for the transfer and use of Passenger Name Record (PNR) data to prevent and combat terrorism and other serious transnational crime (COM(2017) 605 final, 18.10.2017)

2.2.4 European Council

Presidency conclusions of the meeting in Cologne (3-4.6.1999)

Presidency conclusions of the meeting in Nice (7-10.12.2000)

Presidency conclusions of the meeting in Laeken (DOC/01/18, 14-15.12.2001)

The Hague Programme: strengthening freedom, security and justice in the European Union (2005/C 53/01) (OJ C 53, 3.3.2005)

2.2.5 European Parliament

Background note 'EU Passenger Name Record (PNR) directive: an overview' (20150123BKG12902) (1 June 2016)

Legislative Resolution of 7 July 2005 on the proposal for a Council decision on the conclusion of an Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information (API)/Passenger Name Record (PNR) data (COM(2005)0200 – C6-0184/2005 – 2005/0095(CNS)) (P6_TA(2005)0294) (OJ C 157E, 6.7.2006)

Legislative Resolution of 14 April 2016 on the proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011)0032 – C7-0039/2011 – 2011/0023(COD)) (P8_TA(2016)0127) (OJ C 58, 15.2.2018)

Recommendation to the Council of 7 September 2006 on the negotiations for an agreement with the United States of America on the use of passenger name records (PNR) data to prevent and combat terrorism and transnational crime, including organised crime (2006/2193(INI)) (P6_TA(2006)0354) (OJ C 305 E, 14.12.2006)

Recommendation of 22 October 2008 to the Council concerning the conclusion of the Agreement between the European Union and Australia on the processing and transfer of

European Union-sourced passenger name record (PNR) data by air carriers to the Australian customs service (2008/2187(INI)) (P6_TA(2008)0512) (OJ C 15 E, 21.1.2010)

Resolution of 13 March 2003 on transfer of personal data by airlines in the case of transatlantic flights (P5_TA(2003)0097) (OJ C 61 E, 10.3.2004)

Resolution of 9 October 2003 on transfer of personal data by airlines in the case of transatlantic flights: state of negotiations with the USA (P5_TA(2003)0429) (OJ C 81 E, 31.3.2004)

Resolution of 31 March 2004 on the draft Commission decision noting the adequate level of protection provided for personal data contained in the Passenger Name Records (PNRs) transferred to the US Bureau of Customs and Border Protection (2004/2011(INI)) (P5_TA(2004)0245) (OJ C 103 E, 29.4.2004)

Resolution of 14 February 2007 on SWIFT, the PNR agreement and the transatlantic dialogue on these issues (P6_TA(2007)0039) (OJ C 287 E, 29.11.2007)

Resolution of 12 July 2007 on the PNR agreement with the United States of America (P6_TA(2007)0347) (OJ C 175E, 10.7.2008)

Resolution of 20 November 2008 on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes (P6_TA(2008)0561) (OJ C 16E, 22.1.2010)

Resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada (P7_TA(2010)0144) (OJ C 81E, 15.3.2011)

Resolution of 11 November 2010 on the global approach to transfers of passenger name record (PNR) data to third countries, and on the recommendations from the Commission to the Council to authorise the opening of negotiations between the European Union and Australia, Canada and the United States under the EU external strategy on Passenger Name Record (PNR) (P7_TA(2010)0397) (OJ C 74E, 13.3.2012)

Resolution of 25 November 2014 on seeking an opinion from the Court of Justice on the compatibility with the Treaties of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data (2014/2966(RSP)) (P8_TA(2014)0058) (OJ C 289, 9.8.2016)

Resolution of 11 February 2015 on anti-terrorism measures (2015/2530(RSP)) (P8_TA(2015)0032) (OJ C 310, 25.8.2016)

Resolution of 9 July 2015 on the European Agenda on Security (2015/2697(RSP)) (P8_TA(2015)0269) (OJ C 265, 11.8.2017)

Resolution of 25 November 2015 on the prevention of radicalisation and recruitment of European citizens by terrorist organisations (2015/2063(INI)) (P8_TA(2015)0410) (OJ C 366, 27.10.2017)

2.2.6 Multiple institutions

i) Directives

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 (OJ L 281, 23.11.1995)

2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002)

2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (OJ L 158, 30.4.2004)

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 (OJ L 105, 13.4.2006)

(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 (OJ L 119, 4.5.2016)

(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 (OJ L 119, 4.5.2016)

(EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017)

(EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA (OJ L 186, 11.7.2019)

Proposal of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA {SEC(2010) 1122 final} {SEC(2010) 1123 final} (COM(2010) 517 final, 2010/0273 (COD), 30.9.2010)

Proposal of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime {SEC(2011) 132 final} {SEC(2011) 133 final} (COM(2011) 32 final, 2011/0023 (COD), 2.2.2011)

ii) Regulations

(EC) 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 381, 28.12.2006)

(EC) 80/2009 of the European Parliament and of the Council of 14 January 2009 on a Code of Conduct for computerised reservation systems and repealing Council Regulation (EEC) 2299/89 (OJ L 35, 4.2.2009)

(EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ L 77, 23.3.2016)

(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) (OJ L 119, 4.5.2016)

(EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) 45/2001 and Decision 1247/2002/EC (OJ L 295, 21.11.2018)

(EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011 (OJ L 295, 21.11.2018)

(EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018)

2.2.7 Other

Council and Commission Action plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union (2005/C 198/01) (OJ C 198, 12.8.2005)

Joint Statement by First Vice-President Timmermans and Commissioner Avramopoulos on the adoption of the EU Passenger Name Record (PNR) Directive by the European Parliament (STATEMENT/16/1404, 14.4.2016)

Notice from member states on the list of competent authorities referred to in Article 7 of 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 (OJ C 194, 6.6.2018), with the corrigenda

present in OJ C 220, 25.6.2018 and OJ C 344, 26.9.2018

Stockholm Programme — An open and secure Europe serving and protecting citizens (2010/C 115/01) (OJ C 115, 4.5.2010)

Study ‘New technologies: a challenge to privacy protection?’ prepared by the Committee of experts on data protection under the authority of the European Committee on Legal Co-operation (1989)

3. International agreements and policy

Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection attached to the Council Decision of 17 May 2004 (2004/496/EC) (OJ L 183, 20.5.2004)

Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record (OJ L 82, 21.3.2006)

Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security attached to the Council Decision of 16 October 2006 (2006/729/CFSP/JHA) (OJ L 298, 27.10.2006)

Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement) attached to the Council Decision of 23 July 2007 (2007/551/CFSP/JHA) (OJ L 204, 4.8.2007)

Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian customs service attached to the Council Decision 2008/651/CFSP/JHA of 30 June 2008 (OJ L 213, 8.8.2008)

Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service (OJ L 186, 14.7.2012)

Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security attached to the Council Decision of 26 April 2012 (OJ L 215, 11.8.2012)

Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record (12657/5/13 REV 5, 23.6.2014)

Canada-EU Summit joint declaration of 17 and 18 July 2019

Convention on International Civil Aviation (adopted 7 December 1944, entered into force 4 April 1947) 15 UNTS 295 (7300/9)

Joint Statement ‘European Commission/US customs talks on PNR transmission’ (2003)

Letter to the Council Presidency and the Commission from the Department of Homeland Security (DHS) of the United States of America, concerning the interpretation of certain provisions of the undertakings issued by DHS on 11 MAY 2004 in connection with the transfer by air carriers of passenger name record (PNR) data (OJ C 259, 27.10.2006)

Management summary on passenger-related information of the IATA, ICAO, and World Customs Organization (‘Umbrella Document’ version 2.0, July 2017)

Schengen Agreement of 14 June 1985 between the Governments of the states of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders

4. International Air Transport Association

Opinion on the data protection implications of the processing of Passenger Name Records of the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (T-PD(2016)18rev, 19.8.2016)

Resolution on aviation security, adopted at the 73rd IATA annual general meeting (4 to 6 June 2017)

5. International Civil Aviation Organization

Guidelines on Passenger Name Record (PNR) data (9944, 2010)

High-level conference on aviation security working paper on Passenger Name Record (PNR) data and its role in aviation security (HLCAS-WP/5, 4/6/12)

6. Member states of the EU

6.1 Austria

Mitteilung des Ständigen Unterausschusses des Hauptausschusses in Angelegenheiten der Europäischen Union des Nationalrates vom 5. April 2011 gemäß Art. 23f Abs. 4 B-VG

6.2 Germany

Beschlussdes Bundesrates (6007/11)

6.3 The Netherlands

Letter from René van der Linden, president of the Senate of the States General of the Netherlands

7. Third countries

7.1 Australia

Customs Act 1901 (Cth)

Crimes Act 1914 (Cth)

Migration Act 1958 (Cth)

Ombudsman Act 1976 (Cth)

Freedom of Information Act 1982 (Cth)

Customs Administration Act 1985 (Cth)

Privacy Act 1988 (Cth)

Auditor-General Act 1997 (Cth)

Public Service Act 1999 (Cth)

7.2 Canada

Access to Information Act, RSC 1985, c. A-1

Customs Act, RSC 1985, c. 1 (2nd Supp.)

Privacy Act, RSC 1985, c. P-21

Personal Information Protection and Electronic Documents Act, SC 2000, c. 5

Immigration and Refugee Protection Act, SC 2001, c. 27

7.3 United States of America

Code of Federal Regulations

US Code

Privacy Act, Pub. L. 93-579, 88 Stat. 1896 (1974)

Aviation and Transportation Security Act, Pub. L. 107-71, 115 Stat. 597 (2001)

Enhanced Border Security and Visa Entry Reform Act (EBSV), Pub. L. 107-73, 116 Stat. 543 (2002)

Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection, United States Federal Register, volume 69, number 131

B. Cases and opinions

1. European Court of Human Rights

Case *Klass and Others v Germany*, 6 September 1978 (5029/71)

Case *Leander v Sweden*, 26 March 1987 (9248/81)

Case *Kruslin v France*, 24 April 1990 (11801/85)

Case *Kopp v Switzerland*, 25 March 1998 (23224/94)

Case *Amann v Switzerland*, 16 February 2000 (27798/95)

Case *Rotaru v Romania*, 4 May 2000 (28341/95)

Case *Weber and Saravia v Germany*, 29 June 2006 (54934/00)

Case *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*, 28 June 2007 (62540/00)

Case *Liberty and Others v the United Kingdom*, 1 July 2008 (58243/00)

Case *S. and Marper v the United Kingdom*, 4 December 2008 (30562/04 and 30566/04)

Case *B.B., Gardel, and M.B. v France*, 17 December 2009 (5335/06, 16428/05, and 22115/06)

Case *M. K. v France*, 18 April 2013 (19522/09)

Case *Roman Zakharov v Russia*, 4 December 2015 (47143/06)

Case *Szabó and Vissy v Hungary*, 12 January 2016 (37138/14)

2. Court of Justice of the EU

Application in case C-148/20, *Deutsche Lufthansa*, 7 August 2020

Application in case C-149/20, *Deutsche Lufthansa*, 7 August 2020

Application in case C-150/20, *Deutsche Lufthansa*, 7 August 2020

Application in case C-486/20, *Varuh človekovih pravic Republike Slovenije*, 13 November 2020

Joined cases C-7/56 and C-3/57 to C-7/57, *Dinecke Algera, Giacomo Cicconardi, Simone Couturaud, Ignazio Genuardi, Félicie Steichen v Common Assembly of the European Coal and Steel Community*, 12 July 1957 (ECLI:EU:C:1957:7)

Joined cases C-6/69 and 11-69, *Commission of the European Communities v French Republic*, 10 December 1969 (ECLI:EU:C:1969:68)

Case C-41/74, *Yvonne van Duyn v Home Office*, 4 December 1974 (ECLI:EU:C:1974:133)

Case C-36/75, *Roland Rutili v Ministre de l'intérieur*, 28 October 1975 (ECLI:EU:C:1975:137)

Case C-30/77, *Régina v Pierre Bouchereau*, 27 October 1977 (ECLI:EU:C:1977:172)

Case C-120/78, *Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein*, 20 February 1979 (ECLI:EU:C:1979:42)

Case C-148/78, *Criminal proceedings against Tullio Ratti*, 5 April 1979 (ECLI:EU:C:1979:110)

Case C-153/78, *Commission of the European Communities v Federal Republic of Germany*, 12 July 1979 (ECLI:EU:C:1979:194)

Case C-203/80, *Criminal proceedings against Guerrino Casati*, 11 November 1981 (ECLI:EU:C:1981:261)

Case C-72/83, *Campus Oil Limited and others v Minister for Industry and Energy and others*, 10 July 1984 (ECLI:EU:C:1984:256)

Case C-222/84, *Marguerite Johnston v Chief Constable of the Royal Ulster Constabulary*, 15 May 1986 (ECLI:EU:C:1986:206)

Case C-186/87, *Ian William Cowan v Trésor public*, 2 February 1989 (ECLI:EU:C:1989:47)

Case C-300/89, *Commission of the European Communities v Council of the European Communities*, 11 June 1991 (ECLI:EU:C:1991:244)

Case C-367/89, *Criminal proceedings against Aimé Richardt and Les Accessoires Scientifiques SNC*, 4 October 1991 (ECLI:EU:C:1991:376)

Case C-70/94, *Fritz Werner Industrie-Ausrüstungen GmbH v Federal Republic of Germany*, 17 October 1995 (ECLI:EU:C:1995:328)

Case C-83/94, *Criminal proceedings against Peter Leifer, Reinhold Otto Krauskopf and Otto Holzer*, 17 October 1995 (ECLI:EU:C:1995:329)

Case C-226/97, *Criminal proceedings against Johannes Martinus Lemmens*, 16 June 1998 (ECLI:EU:C:1998:296)

Case C-348/96, *Criminal proceedings against Donatella Calfa*, 19 January 1999 (ECLI:EU:C:1999:6)

Case C-42/97, *European Parliament v Council of the European Union*, 23 February 1999 (ECLI:EU:C:1999:81)

Case C-273/97, *Angela Maria Sirdar v The Army Board and Secretary of State for Defence*, 26 October 1999 (ECLI:EU:C:1999:523)

Case C-285/98, *Tanja Kreil v Bundesrepublik Deutschland*, 11 January 2000 (ECLI:EU:C:2000:2)

Case C-54/99, *Association Eglise de scientologie de Paris and Scientology International Reserves Trust v The Prime Minister*, 14 March 2000 (ECLI:EU:C:2000:124)

Case C-423/98, *Alfredo Albore*, 13 July 2000 (ECLI:EU:C:2000:401)

Case C-189/01, *H. Jippes, Afdeling Groningen van de Nederlandse Vereniging tot Bescherming van Dieren and Afdeling Assen en omstreken van de Nederlandse Vereniging tot Bescherming van Dieren v Minister van Landbouw, Natuurbeheer en Visserij*, 12 July 2001 (ECLI:EU:C:2001:420)

Case C-398/98, *Commission of the European Communities v Hellenic Republic*, 25 October 2001 (ECLI:EU:C:2001:565)

Joined cases C-27/00 and C-122/00, *The Queen v Secretary of State for the Environment, Transport and the Regions, ex parte Omega Air Ltd (C-27/00) and Omega Air Ltd, Aero Engines Ireland Ltd and Omega Aviation Services Ltd v Irish Aviation Authority (C-122/00)*, 12 March 2002 (ECLI:EU:C:2002:161)

Case C-336/00, *Republik Österreich v Martin Huber*, 19 September 2002 (ECLI:EU:C:2002:509)

Case C-186/01, *Alexander Dory v Bundesrepublik Deutschland*, 11 March 2003 (ECLI:EU:C:2003:146)

Joined cases C-465/00, C-138/01 and C-139/01, *Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v Österreichischer Rundfunk*, 20 May 2003 (ECLI:EU:C:2003:294)

Case C-112/00, *Eugen Schmidberger, Internationale Transporte und Planzüge v Republik Österreich*, 12 June 2003 (ECLI:EU:C:2003:333)

Case C-252/01, *Commission of the European Communities v Kingdom of Belgium*, 16 October 2003 (ECLI:EU:C:2003:547)

Case C-36/02, *Omega Spielhallen- und Automatenaufstellungs-GmbH v Oberbürgermeisterin der Bundesstadt Bonn*, 14 October 2004 (ECLI:EU:C:2004:614)

Case C-105/03, *Criminal proceedings against Maria Pupino*, 16 June 2005 (ECLI:EU:C:2005:386)

Case C-504/04, *Agrarproduktion Staebelow GmbH v Landrat des Landkreises Bad Doberan*, 12 January 2006 (ECLI:EU:C:2006:30)

Joined cases C-317/04, *European Parliament v Council of the European Union*, and C-318/04, *European Parliament v Commission of the European Communities*, 30 May 2006 (ECLI:EU:C:2006:346)

Case C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU*, 29 January 2008 (ECLI:EU:C:2008:54)

Case C-337/05, *Commission of the European Communities v Italian Republic*, 8 April 2008 (ECLI:EU:C:2008:203)

Case C-33/07, *Ministerul Administrației și Internelor – Direcția Generală de Pașapoarte București v Gheorghe Jipa*, 10 July 2008 (ECLI:EU:C:2008:396)

Case C-402/05 P and C-415/05 P, *Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities*, 3 September 2008 (ECLI:EU:C:2008:461)

Case C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*, 16 December 2008 (ECLI:EU:C:2008:727)

Case C-558/07, *The Queen, on the application of S.P.C.M. SA, C.H. Erbslöh KG, Lake Chemicals and Minerals Ltd and Hercules Inc. v Secretary of State for the Environment, Food and Rural Affairs*, 7 July 2009 (ECLI:EU:C:2009:430)

Case C-387/05, *European Commission v Italian Republic*, 15 December 2009 (ECLI:EU:C:2009:781)

Case C-461/05, *European Commission v Kingdom of Denmark*, 15 December 2009 (ECLI:EU:C:2009:783)

Case C-38/06, *European Commission v Portuguese Republic*, 4 March 2010 (ECLI:EU:C:2010:108)

Case C-518/07, *European Commission v Federal Republic of Germany*, 9 March 2010 (ECLI:EU:C:2010:125)

Joined cases C-379/08 and C-380/08, *Raffinerie Mediterranée (ERG) SpA, Polimeri Europa SpA and Syndial SpA v Ministero dello Sviluppo economico and Others (C-379/08) and ENI SpA v Ministero Ambiente e Tutela del Territorio e del Mare and Others (C-380/08)*, 9 March 2010 (ECLI:EU:C:2010:127)

Case C-58/08, *The Queen, on the application of Vodafone Ltd and Others v Secretary of State for Business, Enterprise and Regulatory Reform*, 8 June 2010 (ECLI:EU:C:2010:321)

Case C-343/09, *Afton Chemical Limited v Secretary of State for Transport*, 8 July 2010 (ECLI:EU:C:2010:419)

Joined cases C-92/09 e C-93/09, *Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen*, 9 November 2010 (ECLI:EU:C:2010:662)

Case C-145/09, *Land Baden-Württemberg v Panagiotis Tsakouridis*, 23 November 2010 (ECLI:EU:C:2010:708)

Case C-61/11 PPU, *Hassen El Dridi, alias Soufi Karim*, 28 April 2011 (ECLI:EU:C:2011:268)

Case C-543/09, *Deutsche Telekom AG v Bundesrepublik Deutschland*, 5 May 2011 (ECLI:EU:C:2011:279)

Case C-430/10, *Hristo Gaydarov v Direktor na Glavna direktsia 'Ohranitelna politsia' pri Ministerstvo na vatreshnite raboti*, 17 November 2011 (ECLI:EU:C:2011:749)

Case C-434/10, *Petar Aladzhov v Zamestnik direktor na Stolichna direktsia na vatreshnite raboti kam Ministerstvo na vatreshnite raboti*, 17 November 2011 (ECLI:EU:C:2011:750)

Joined cases C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) v Administración del Estado*, 24 November 2011 (ECLI:EU:C:2011:777)

Case C-348/09, *P.I. v Oberbürgermeisterin der Stadt Remscheid*, 22 May 2012 (ECLI:EU:C:2012:300)

Case C-278/12 PPU, *Atiqullah Adil v Minister voor Immigratie, Integratie en Asiel*, 19 July 2012 (ECLI:EU:C:2012:508)

Case C-614/10, *European Commission v Republic of Austria*, 16 October 2012 (ECLI:EU:C:2012:631)

Joined cases C-581/10 and C-629/10, *Emeka Nelson and Others v Deutsche Lufthansa AG and TUI Travel plc and Others v Civil Aviation Authority*, 23 October 2012 (ECLI:EU:C:2012:657)

Joined cases C-539/10 P and C-550/10 P, *Stichting Al-Aqsa v Council of the European Union and Kingdom of the Netherlands v Stichting Al-Aqsa*, 15 November 2012 (ECLI:EU:C:2012:711)

Case C-283/11, *Sky Österreich GmbH v Österreichischer Rundfunk*, 22 January 2013 (ECLI:EU:C:2013:28)

Case C-300/11, *ZZ v Secretary of State for the Home Department*, 4 June 2013 (ECLI:EU:C:2013:363)

Case C-101/12, *Herbert Schaible v Land Baden-Württemberg*, 17 October 2013 (ECLI:EU:C:2013:661)

Case C-291/12, *Michael Schwarz v Stadt Bochum*, 17 October 2013 (ECLI:EU:C:2013:670)

Case C-473/12, *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and Others*, 7 November 2013 (ECLI:EU:C:2013:715)

Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014 (ECLI:EU:C:2014:238)

Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 13 May 2014 (ECLI:EU:C:2014:317)

Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015 (ECLI:EU:C:2015:650)

Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, 21 December 2016 (ECLI:EU:C:2016:970)

Case C-9/16, *Criminal proceedings against A*, 21 June 2017 (ECLI:EU:C:2017:483)

Case C-178/16, *European Commission v Republic of Austria*, 20 March 2018 (ECLI:EU:C:2018:194)

Joined cases C-715/17, C-718/17 and C-719/17, *European Commission v Republic of Poland and Others*, 2 April 2020 (ECLI:EU:C:2020:257)

Case C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*, 6 October 2020 (ECLI:EU:C:2020:790)

Joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others v Premier ministre and Others*, 6 October 2020 (ECLI:EU:C:2020:791)

Case C-808/18, *European Commission v Hungary*, 17 December 2020 (ECLI:EU:C:2020:1029)

Opinion 2/00, delivered on 6 December 2001 (ECLI:EU:C:2001:664)

Opinion 1/15, delivered on 26 July 2017 (ECLI:EU:C:2017:592)

Request for a preliminary ruling in case C-817/19, *Ligue des droits humains*, 31 October 2019

Request for a preliminary ruling in case C-215/20, *Bundesrepublik Deutschland*, 19 May 2020

Request for a preliminary ruling in case C-222/20, *Bundesrepublik Deutschland*, 27 May 2020

Opinion of Advocate General Francis Jacobs, delivered on 18 May 1995 (ECLI:EU:C:1995:151)

Opinion of Advocate General Juliane Kokott, delivered on 11 November 2004 (ECLI:EU:C:2004:712)

Opinion of Advocate General Philippe Léger, delivered on 22 November 2005 (ECLI:EU:C:2005:710)

Opinion of Advocate General Pedro Cruz Villalón, delivered on 12 December 2013 (ECLI:EU:C:2013:845)

Opinion of Advocate General Juliane Kokott, delivered on 31 May 2016 (ECLI:EU:C:2016:382)

Opinion of Advocate General Paolo Mengozzi, delivered on 8 September 2016 (ECLI:EU:C:2016:656)

Opinion of Advocate General Manuel Campos Sánchez-Bordona, delivered on 15 January 2020 (ECLI:EU:C:2020:5)

Opinion of Advocate General Manuel Campos Sánchez-Bordona, delivered on 15 January 2020 (ECLI:EU:C:2020:6)

3. Other courts

Judgment of the Polish Constitutional Court, *Poland's membership in the European Union (the Accession Treaty)*, 11 May 2005 (K 18/04)

Judgment of the Second Senate of the German Constitutional Court, *Lisbon*, 2 BvE 2/08, 30 June 2009 (ECLI:DE:BVerfG:2009:es20090630.2bve000208)

C. Opinions from advisory and supervisory bodies of the EU

1. The Article 29 Working Party

Letter to Dimitris Avramopoulos, Commissioner for Migration, Home Affairs and Citizenship, on PNR obligations Mexico, dated from 6 February 2015

Letter to Claude Moraes, Chairman of the LIBE Committee of the European Parliament, on EU PNR, dated from 19 March 2015 (Ref. Ares(2015)1241920)

Opinion 2/2001 of Article 29 Working Party, adopted on 26 January 2001, on the adequacy of the Canadian Personal Information and Electronic Documents Act (5109/00/EN, WP 39)

Opinion 6/2002, adopted on 24 October 2002, on transmission of Passenger Manifest Information and other data from Airlines to the United States (11647/02/EN, WP 66)

Opinion 4/2003, adopted on 13 June 2003, on the level of protection ensured in the US for the transfer of passengers' data (11070/03/EN, WP 78)

Opinion 1/2004, adopted on 16 January 2004, on the level of protection ensured in Australia for the transmission of Passenger Name Record data from airlines (10031/03/EN, WP 85)

Opinion 2/2004, adopted on 29 January 2004, on the adequate protection of personal data contained in the PNR of air passengers to be transferred to the United States' Bureau of Customs and Border Protection (US CBP) (10019/04/EN, WP 87)

Opinion 3/2004, adopted on 11 February 2004, on the level of protection ensured in Canada for the transmission of Passenger Name Records and Advanced Passenger Information from airlines (10037/04/EN, WP 88)

Opinion 6/2004, adopted on 22 June 2004, on the implementation of the Commission decision of 14-V-2004 on the adequate protection of personal data contained in the Passenger Name Records of air passengers transferred to the United States' Bureau of Customs and Border

Protection, and of the Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (11221/04/EN, WP 95)

Opinion 8/2004, adopted on 30 September 2004, on the information for passengers concerning the transfer of PNR data on flights between the European Union and the United States of America (11733/04/EN, WP 97)

Opinion 10/2004, adopted on 25 November 2004, on more harmonised information provisions (11987/04/EN, WP 100)

Opinion 1/2005, adopted on 19 January 2005, on the level of protection ensured in Canada for the transmission of Passenger Name Record and Advance Passenger Information from airlines (1112/05/EN, WP 103)

Opinion 5/2006, adopted on 14 June 2006, on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States (1015/06/EN, WP 122)

Opinion 7/2006, adopted on 27 September 2006, on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States and the urgent need for a new agreement (1612/06/EN, WP 124)

Opinion 9/2006, adopted on 27 September 2006, on the implementation of Directive 2004/82/EC of the Council on the obligation of carriers to communicate advance passenger data (1613/06/EN, WP 127)

Opinion 2/2007, adopted on 15 February 2007, on information to passengers about transfer of PNR data to US authorities (XXXX/07/EN, WP132)

Opinion 5/2007, adopted on 17 August 2007, on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007 (01646/07/EN, WP 138)

Opinion 7/2010, adopted on 12 November 2010, on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries (622/10/EN, WP 178)

Opinion 10/2011, adopted on 5 April 2011, on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (00664/11/EN, WP 181)

Joint opinion of the Article 29 Data Protection Working Party (145, 5.12.2007) and the Working Party on Police and Justice (01/07, 18.12.2007) on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007 (02422/07/EN)

Recommendation 1/98, adopted on 28 April 1998, on airline Computerised Reservation Systems (CRS) (XV D/5009/98 final, WP 10)

Working document, adopted on 14 September 2001, on IATA Recommended Practice 1774 'Protection for privacy and transborder data flows of personal data used in international air transport of passengers and of cargo' (5032/01/EN/Final, WP 49)

Working document, adopted on 25 November 2005, on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (2093/05/E, WP 114)

2. Committee of the Regions

Agenda item 4: Organisation of future work — decisions not to draw up opinions, adopted by the CIVEX, on 8 April 2011 (CdR 119/2011 EN/o)

Agenda item 5a): Organisation of COR commission work — referrals made by the COR president, adopted by the COR at its 129th meeting, on 30 March 2011 (R/CdR 91/2011 item 5a) FR/CD/ym)

Opinion on the EU internal security strategy (CIVEX-V-018, 1.7.2011)

3. European Data Protection Supervisor

Opinion on the proposal for a Council Decision on the conclusion of an agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information (API) / Passenger Name Record (PNR) data (OJ C 218, 6.9.2005)

Opinion on the draft proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes (OJ C 110, 1.5.2008)

Opinion on the Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries (OJ C 357, 30.12.2010)

Opinion on the proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (2011/C 181/02) (OJ C 181, 22.6.2011)

Opinion on the proposal for a Council decision on the conclusion of an Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service (OJ C 322, 5.11.2011)

Opinion on the proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security (OJ C 35, 9.2.2012)

Opinion on the proposals for Council decisions on the conclusion and the signature of the agreement between Canada and the European Union on the transfer and processing of passenger name record data (OJ C 51, 22.2.2014)

Opinion 5/2015 ‘Second opinion on the proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime’ (OJ C 392, 25.11.2015)

STATEMENT EDPS/2015/12 (10.12.2015)

4. European Economic and Social Committee

Opinion on the Proposal for a regulation of the European Parliament and of the Council on a Code of conduct for computerised reservation systems (COM(2007) 709 final — 2007/0243 (COD)) (2008/C 224/12) (OJ C 224, 30.8.2008)

Opinion on the ‘Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime’ (COM(2011) 32 final — 2011/0023 (COD)) (2011/C 218/20) (OJ C 218, 23.7.2011)

5. Fundamental Rights Agency

Fundamental Rights Report 2017

2008 Opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes

Opinion 1/2011 on the Proposal for a Directive on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011) 32 final)

2014 Twelve operational fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data

D. Bibliography

Access Now, 2016. *The stormy seas of privacy in Europe*. Available at: <https://www.accessnow.org/stormy-seas-privacy-europe/> (accessed on 10 July 2020)

Adele, 2015. *Hello*. 25

Alston, P. & Weiler, J., 1998. An 'ever closer Union' in need of a human rights policy. *European Journal of International Law*, 9(4), pp. 658-723

Amadeus, 2018. 1987. Available at: http://www.amadeus.com/web/amadeus/en_1A-corporate/Amadeus-Home/About-us/Our-history/1987-New-global-distribution-system/1319591612325-Page-AMAD_DetailPpal?assetid=1319593241232&assettype=StandardContent_C (accessed on 1 June 2018)

Amato, G. & Ziller, J., 2007. *The European Constitution: Cases and materials in EU and member states' law*. Cheltenham: Edward Elgar

Argomaniz, J., 2009. When the EU is the 'norm-taker': The Passenger Name Records agreement and the EU's internalization of US border security norms. *Journal of European Integration*, 31(1), pp. 119-136

Attanasio, J., 2002. Security for the future: Let's get our airlines flying. *Journal of Air Law and Commerce*, 67(1), pp. 9-27

Azoulai, L., 2011. The 'retained powers' formula in the case law of the European Court of Justice: EU law as total law. *European Journal of Legal Studies*, 4(2), pp. 192-219

Baldaccini, A. & Toner, H., 2007. From Amsterdam and Tampere to The Hague: An overview of five years of EC immigration and asylum law. In: A. Baldaccini, E. Guild & H. Toner, eds. *Whose freedom, security and justice?* Oxford: Hart Publishing, pp. 1-22

Barros, X., 2012. The external dimension of EU counter-terrorism: The challenges of the European Parliament in front of the European Court of Justice. *European Security*, 21(4), pp. 518-536

BBC,

2015 (a). *Charlie Hebdo attack: 12 dead at French magazine offices*. Available at: <https://www.bbc.com/news/av/world-europe-30712020> (accessed on 4 March 2021)

2015 (b). *Paris attacks: What happened on the night*. Available at: <https://www.bbc.com/news/world-europe-34818994> (accessed on 4 March 2021)

2016. *Brussels attacks: Zaventem and Maelbeek bombs kill many*. Available at: <https://www.bbc.com/news/world-europe-35869254> (accessed on 4 March 2021)

Bellanova, R., 2014. Data protection, with love. *International Political Sociology*, 8(1), pp. 112-115

Bellanova, R. & Duez, D., 2013. Le citoyen face aux nouvelles pratiques sécuritaires de l'Union européenne: Enjeux démocratiques d'une sécurité par les fichiers. *Espace populations sociétés*, Volume 2012-3, pp. 49-62

Benedizione, L. & Paris, E., 2015. Preliminary reference and dialogue between courts as tools for reflection on the EU system of multilevel protection of rights: The case of the data retention Directive. *German Law Journal*, 16(6), pp. 1727-1769

Bignami, F., 2007. Privacy and law enforcement in the European Union: The data retention directive. *Chicago Journal of International Law*, 8(1), pp. 233-256

Bigo, D., Carrera, S., Guild, E. & Mitsilegas, V., 2016. *The EU and the 2016 Terrorist Attacks in Brussels: Better instead of more information sharing*. Available at: <https://www.ceps.eu/ceps-publications/eu-and-2016-brussels-terrorist-attacks-better-instead-more-information-sharing/> (accessed on 23 April 2021)

Bigo, D. et al., 2015. The EU counter-terrorism policy responses to the attacks in Paris: Towards an EU security and liberty agenda. *CEPS Papers in Liberty and Security in Europe*, Volume 81, pp. 1-18

Bîrzu, B., 2016. Prevention, detection, investigation and prosecution of terrorist offenses and other serious crimes by using Passenger Name Record (PNR) data. Critical opinions. De lege ferenda proposals. *Perspectives of Business Law Journal*, 5(1), pp. 195-206

Blanke, H.-J., 2013. Article 4 [The relations between the EU and the member states] (ex-Article 6.3, 33 TEU, ex-Article 10 EC). In: H. Blanke & S. Mangiameli, eds. *The Treaty on European Union (TEU). A commentary*. Heidelberg: Springer, pp. 185-253

Borriello, F., 2020. Principle of proportionality and the principle of reasonableness. *Review of European Administrative Law*, 13(2), pp. 155-174

Bossong, R., 2017. *Passenger Name Records – from Canada back to the EU*. Available at: <https://verfassungsblog.de/passenger-name-records-from-canada-back-to-the-eu/> (accessed on 28 May 2020)

Bug, M. & Bukow, S., 2017. Civil liberties vs. security: Why citizens accept or reject digital security measures. *German Politics*, 26(2), pp. 292-313

Calders, T. & Zliobaite, I., 2013. Why unbiased computational processes can lead to discriminative decision procedures. In: B. Custers, T. Calders, B. Schermer & T. Zarsky, eds. *Discrimination and privacy in the information society. Data mining and profiling in large databases*. Berlin: Springer, pp. 43-57

Cantaro, A., 2006. Il rispetto delle funzioni essenziali dello Stato. In: S. Mangiameli, ed. *L'ordinamento Europeo. I principi dell'Unione*. Milan: Giuffrè Editore, pp. 507-565

Carpanelli, E. & Lazzarini, N., 2017. PNR: Passenger Name Record, Problems Not Resolved? The EU PNR conundrum after Opinion 1/15 of the CJEU. *Air & Space Law*, 42(4-5), pp. 377-402

- Casagran, C., 2015. The future EU PNR system: Will passenger data be protected? *European Journal of Crime, Criminal Law and Criminal Justice*, 23(3), pp. 241-257
- Chandler, J., 2009. Privacy versus national security: Clarifying the trade-off. In: I. Kerr, V. Steeves & C. Lucock, eds. *Lessons from the identity trail, anonymity, privacy and identity in a networked society*. Oxford: Oxford University Press, pp. 121-138
- Chiappetta, A. & Battaglia, A., 2018. The impact of privacy and cybersecurity on e-record: The PNR Directive adoption and the impact of GDPR. *Journal of Sustainable Development of Transport and Logistics*, 3(3), pp. 77-87
- Council of the European Union, 2020. *EU-Japan PNR agreement: Council authorises opening of negotiations*. Available at: <https://www.consilium.europa.eu/en/press/press-releases/2020/02/18/eu-japan-pnr-agreement-council-authorises-opening-of-negotiations/> (accessed on 25 May 2020)
- Craig, P., 2010. *The Lisbon Treaty: Law, politics, and Treaty reform*. Revised Edition. Oxford: Oxford University Press
- Craig, P. & De Búrca, G., 2015. *EU law: Text, cases, and materials*. 6th edition. Oxford: Oxford University Press
- Cremona, M., 2006. *External relations of the EU and the member states: Competence, mixed agreements, international responsibility, and effects of international law*. San Domenico di Fiesole: European University Institute
- De Goede, M., 2012. *Speculative security: The politics of pursuing terrorist monies*. Minneapolis: University of Minnesota Press
- De Hert, P. & Bellanova, R., 2011. Mobility should be fun. A consumer (law) perspective on border check technology. *The Scientific World Journal*, Volume 11, pp. 490-502
- De Hert, P. & Papakonstantinou, V., 2015. Editorial. Repeating the mistakes of the past will do little good for air passengers in the EU. *New Journal of European Criminal Law*, 6(2), pp. 160-165
- De Witte, B., 2017. Exclusive member state competences — Is there such a thing? In: S. Garben & I. Govaere, eds. *The division of competences between the EU and the member states: Reflections on the past, the present and the future*. Oxford: Hart Publishing, pp. 59-73
- Di Matteo, F., 2017. La raccolta indiscriminata e generalizzata di dati personali: Un vizio congenito nella direttiva PNR? *Diritti Umani e Diritto Internazionale*, Volume 1, pp. 213-236
- Dimitropoulos, G., 2015. The CJEU's decision on the data retention Directive: Transnational aspects and the push for harmonisation — A comment on professor Martin Nettesheim. In: B. Hess & C. Mariottini, eds. *Protecting privacy in private international and procedural law and by data protection: European and American Developments*. Baden-Baden: Nomos, pp. 71-79

Directorate-General for internal policies of the European Parliament, 2014. *National security and secret evidence in legislation and before the courts: Exploring the challenges*, Brussels: European Parliament

Dobbs, M., 2014. Sovereignty, article 4(2) TEU and the respect of national identities: Swinging the balance of power in favour of the member states? *Yearbook of European Law*, 33(1), pp. 298-334

Docksey, C., 2016. Four fundamental rights: Finding the balance. *International Data Privacy Law*, 6(3), pp. 195-209

Dougan, M., 2008. The Treaty of Lisbon 2007: Winning minds, not hearts. *Common Market Law Review*, 45(3), pp. 617-703

Electronic Frontier Foundation, 2014. *Necessary & proportionate. International principles on the application of human rights law to communications surveillance*

Encyclopaedia Britannica, 2020. *National security*. Available at: <https://www.britannica.com/topic/national-security> (accessed on 1 October 2020)

Enerstvedt, O.,

2014. Russian PNR system: Data protection issues and global prospects. Volume 30, pp. 25-40

2017. *Aviation security, privacy, data protection and other human rights: Technologies and legal principles*. Cham: Springer

European Commission,

2010. *Commission presents a new set of EU measures to better protect European citizens (IP/10/1535)*. Available at: http://europa.eu/rapid/press-release_IP-10-1535_en.htm?locale=fr (accessed on 22 October 2018)

2011. *EU Passenger Name Record (PNR) - Frequently Asked Questions (MEMO/11/60)*, Brussels

2021. *Distribution networks - CRS*. Available at: https://ec.europa.eu/transport/modes/air/internal-market/distribution-networks-crs_en (accessed on 18 May 2021)

2021. *Passenger Name Record (PNR)*. Available at: https://ec.europa.eu/home-affairs/what-we-do/policies/law-enforcement-cooperation/information-exchange/pnr_en (accessed on 21 April 2021)

European Data Protection Supervisor, 2021. *Search*. Available at: https://edps.europa.eu/search_en?search=pnr (accessed on 23 April 2021)

European Parliament, 2018. *Public security exception in the area of non-personal data in the European Union*, Brussels: European Parliament

European Parliamentary Research Service,

2015. *The proposed EU passenger name records (PNR) directive. Revived in the new security context*, European Parliament

2016. *Completing the adoption of an EU PNR Directive*, Brussels: European Parliament

European Union Committee of the House of Lords, 2008. *The Treaty of Lisbon: An impact assessment (10th report of session 2007-08)*, London: The Stationery Office Limited

Eurostat,

2021. *International extra-EU air passenger transport by reporting country and partner world regions and countries*. Available at: https://ec.europa.eu/eurostat/databrowser/view/AVIA_PAEXCC_custom_980487/default/table?lang=en (accessed on 21 May 2021)

2021. *International intra-EU air passenger transport by reporting country and EU partner country*. Available at: https://ec.europa.eu/eurostat/databrowser/view/AVIA_PAINCC_custom_980497/default/table?lang=en (accessed on 21 May 2021)

Fabbrini, F., 2015. Human rights in the digital age: The European Court of Justice ruling in the data retention case and its lessons for privacy and surveillance in the United States. *Harvard Human Rights Journal*, 28(1), pp. 65-95

Faull, J., 2011. The role of the European Commission in tackling terrorism: The example of Passenger Name Records. In: A. Arnall, C. Barnard, M. Dougan & E. Spaventa, eds. *A constitutional order of states?: Essays in EU Law in honour of Alan Dashwood*. London: Hart Publishing, pp. 609-620

Fennelly, D., 2019. Data retention: The life, death and afterlife of a directive. *ERA Forum*, 19(4), pp. 673-692

Gandy, O., 2010. Engaging rational discrimination: Exploring reasons for placing regulatory constraints on decision support systems. *Ethics and Information Technology*, 12(1), pp. 29-42

Garben, S., 2015. Confronting the competence conundrum: Democratising the European Union through an expansion of its legislative powers. *Oxford Journal of Legal Studies*, 35(1), pp. 55-89

Gilbert, N., 2007. Dilemmas of privacy and surveillance: Challenges of technological change. *Criminal Justice Matters*, 68(1), pp. 41-42

Gillespie, T., 2014. The relevance of algorithms. In: T. Gillespie, P. Boczkowski & K. Foot, eds. *Media technologies: Essays on communication, materiality, and society*. Cambridge: MIT Press, pp. 167-194

- Granger, M.-P. & Irion, K., 2014. The Court of Justice and the data retention Directive in Digital Rights Ireland: Telling off the EU legislator and teaching a lesson in privacy and data protection. *European Law Review*, 39(6), pp. 835-850
- Hampton, M., 2013. *A thorn in transatlantic relations: American and European perceptions of threat and security*. New York: Palgrave Macmillan
- Han, C.-R., McGaurana, R. & Nelen, H., 2017. API and PNR data in use for border control authorities. *Security Journal*, 30(4), pp. 1045-1063
- Harding, C., 2015. EU criminal law under the area of freedom, security, and justice. In: D. Chalmers & A. Arnall, edits. *The Oxford handbook of European Union law*. Oxford: Oxford University Press, pp. 1-30
- Hartley, T., 2014. *The foundations of European Union law*. 8th edition. Oxford: Oxford University Press
- Hijmans, H., 2017. PNR Agreement EU-Canada scrutinised: CJEU gives very precise guidance to negotiators. *European Data Protection Law Review*, 3(3), pp. 406-412
- Hijmans, H. & Scirocco, A., 2009. Shortcomings in EU data protection in the third and the second pillars. Can the Lisbon Treaty be expected to help? *Common Market Law Review*, 46(5), pp. 1485-1525
- Hildebrant, M. & Gutwirth, S., 2008. Concise conclusions: Citizens out of control. In: *Profiling the European citizen: Cross-disciplinary perspectives*. Dordrecht: Springer, pp. 365-368
- Hodgson, C. & Waldmeir, P., 2018. *How airlines aim to use big data to boost profits*. Available at: <https://www.ft.com/content/f3a931be-47aa-11e8-8ae9-4b5ddcca99b3> (accessed on 2 May 2019)
- Hoofnagle, C., Van der Sloot, B. & Borgesius, F., 2019. The European Union general data protection regulation: What it is and what it means. *Information & Communications Technology Law*, 28(1), pp. 65-98
- Huijboom, N. & Bodea, G., 2015. Understanding the political PNR debate in Europe: A discourse analytical perspective. *European Politics and Society*, 16(2), pp. 241-255
- Isserow, J. & Klein, C., 2017. Hypocrisy and moral authority. *Journal of Ethics and Social Philosophy*, 12(2), pp. 191-222
- Jones, B., 2011. *Franco-British military cooperation: A new engine for European defence?* Paris: European Union Institute for Security Affairs
- Jones, C., 2012. *Statewatch analysis: Making fundamental rights flexible*. Available at: <https://www.statewatch.org/media/documents/analyses/no-169-eu-pnr-us-aus-comparison.pdf> (accessed on 13 April 2021)

Kargopoulos, A., 2016. Fundamental rights, national identity and EU criminal law. In: V. Mitsilegas, M. Bergström & T. Konstadinides, eds. *Research handbook on EU criminal law*. Cheltenham: Edward Elgar, pp. 125-147

Kellerbauer, M., 2019. Article 72 TFEU. In: M. Kellerbauer, M. Klamert & J. Tomkin, eds. *Commentary on the EU treaties and the Charter of Fundamental Rights*. Oxford: Oxford University Press, p. 791

Kirkhope, T., 2015. *PNR key tool for tackling major criminality* [interview] (2 February 2015). Available at: https://www.youtube.com/watch?v=jq_I5YT2KDY (accessed on 10 October 2018)

Klamert, M.,

2019 (a). Title I. Common provisions. In: M. Kellerbauer, M. Klamert & J. Tomkin, eds. *Commentary on the EU treaties and the Charter of Fundamental Rights*. Oxford: Oxford University Press, pp. 5-6

2019 (b). Article 4 TEU. In: M. Kellerbauer, M. Klamert & J. Tomkin, eds. *Commentary on the EU treaties and the Charter of Fundamental Rights*. Oxford: Oxford University Press, pp. 35-60

Klip, A., 2016. *European criminal law. An integrative approach*. 3rd edition. Cambridge: Intersentia

Kokott, J. & Sobotta, C., 2013. The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, 3(4), pp. 222-228

Kolliarakis, G., 2017. In quest of reflexivity. Towards an anticipatory governance regime for security. In: M. Friedewald, et al. eds. *Surveillance, privacy and security. Citizens' perspectives*. Abingdon: Routledge, pp. 233-254

Kuner, C.,

2017. *Data protection, data transfers, and international agreements: The CJEU's Opinion 1/15*. Available at: <https://verfassungsblog.de/data-protection-data-transfers-and-international-agreements-the-cjeus-opinion-115/> (accessed on 28 May 2020)

2018. International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR. *Common Market Law Review*, 55(3), pp. 857-882

2019. The internet and the global reach of EU law. In: M. Cremona & J. Scott, eds. *EU law beyond EU borders: The extraterritorial reach of EU law*. Oxford: Oxford University Press, pp. 112-145

Labayle, H., 2016. The institutional framework. In: V. Mitsilegas, M. Bergström & T. Konstadinides, eds. *Research handbook on EU criminal law*. Cheltenham: Edward Elgar, pp. 29-48

Ladenburger, C., 2008. Police and criminal law in the Treaty of Lisbon. A new dimension for the Community method. *European Constitutional Law Review*, 4(1), pp. 20-40

Leczykiewicz, D., 2019. The Charter of Fundamental Rights and the EU's shallow constitutionalism. In: N. Barber, M. Cahill & R. Ekins, eds. *The rise and fall of the European constitution*. Oxford: Hart Publishing, pp. 125-154

Leese, M., 2014. The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. *Security Dialogue*, 45(5), pp. 494-511

Lenaerts, K.,

1990. Constitutionalism and the many faces of federalism. *The American Journal of Comparative Law*, 38(2), pp. 205-263

2012. Exploring the limits of the EU Charter of Fundamental Rights. *European Constitutional Law Review*, 8(3), pp. 375-403

Loideain, N., 2015. EU law and mass internet metadata surveillance in the post-Snowden era. *Media and Communication*, 3(2), pp. 53-62

Lord, B., 2019. The protection of personal data in international civil aviation: The transatlantic clash of opinions. *Air & Space Law*, 44(3), pp. 261-274

Lowe, D., 2016. The European Union's Passenger Name Record Data Directive 2016/681: Is it fit for purpose? *International Criminal Law Review*, Volume 16, pp. 856-884

Lund, J., 2017. *Danish Defence Intelligence Service will get access to PNR data*. Available at: <https://edri.org/danish-defence-intelligence-service-will-get-access-to-pnr-data/> (accessed on 10 October 2018)

Lynskey, O.,

2014. The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland. *Common Market Law Review*, 51(6), pp. 1789-1812

2015. *The foundations of EU data protection law*. Oxford: Oxford University Press

Maduro, M., 2003. The double constitutional life of the Charter of Fundamental Rights in the European Union. In: T. Hervey & J. Kenner, eds. *Economic and social rights under the EU Charter of Fundamental Rights. A legal perspective*. London: Hart Publishing, pp. 269-300

Manrique de Luna Barrios, A., 2017. The European Union as an international actor of peace and security. In: B. Pérez de las Heras, ed. *Democratic legitimacy in the European Union and global governance: Building a European demos*. Cham: Palgrave Macmillan, pp. 305-319

Maras, M.-H., 2012. The social consequences of a mass surveillance measure: What happens when we become the 'others'? *International Journal of Law, Crime and Justice*, 40(2), pp. 65-81

Marin, L., 2016. The fate of the data retention Directive: About mass surveillance and fundamental rights in the EU legal order. In: V. Mitsilegas, M. Bergström & T. Konstadinides, eds. *Research handbook on EU criminal law*. Cheltenham: Edward Elgar, pp. 210-229

Massé, E. & Krahulcova, L., 2016. *The stormy seas of privacy in Europe*. Available at: <https://www.accessnow.org/stormy-seas-privacy-europe/> (accessed on 11 April 2019)

Mattli, W. & Woods, N., 2009. In whose benefit? Explaining regulatory change in global politics. In: W. Mattli & N. Woods, eds. *The politics of global regulation*. Princeton: Princeton University Press, pp. 15-48

McCue, C., 2015. *Data mining and predictive analysis: Intelligence gathering and crime analysis*. 2nd edition. Oxford: Elsevier

McKeever, D., 2021. Revisiting Security Council action on terrorism: New threats; (a lot of) new law; same old problems? *Leiden Journal of International Law*, pp. 1-30

Mendes de Leon, P., 2017. *Introduction to Air Law*. Alphen aan den Rijn: Kluwer Law

Mendez, M., 2017. Opinion 1/15: The Court of Justice meets PNR data (again!). *European Papers*, 2(3), pp. 803-818

Mitsilegas, V.,

2010. European criminal law and resistance to communitarisation after Lisbon. *New Journal of European Criminal Law*, 1(4), pp. 458-480

2015. The transformation of privacy in an era of pre-emptive surveillance. *Tilburg Law Review*, Volume 20, pp. 35-57

2017. The security Union as a paradigm of preventive justice: Challenges for citizenship, fundamental rights and the rule of law. In: S. Carrera & V. Mitsilegas, eds. *Constitutionalising the security Union. Effectiveness, rule of law and rights in countering terrorism and crime*. Brussels: CEPS, pp. 5-20

Molina del Pozo, C. & Mata Diz, J., 2013. La distribución de competencias en el nuevo diseño de la Unión Europea: Del Acta Única Europea al Tratado de Lisboa. *Revista Facultad de Derecho y Ciencias Políticas*, 43(118), pp. 15-59

Möller, K., 2014. Constructing the proportionality test: An emerging global conversation. In: L. Lazarus, C. McCrudden & N. Bowles, eds. *Reasoning rights: Comparative judicial engagement*. Oxford: Hart Publishing, pp. 31-40

Monar, J., 2011. The Area of Freedom, Security and Justice. In: A. Von Bogdandy & J. Bast, eds. *Principles of European constitutional law*. 2nd revised edition. Oxford: Hart Publishing, pp. 551-585

Moore, A., 2011. Privacy, security, and government surveillance: Wikileaks and the new accountability. *Public Affairs Quarterly*, 25(2), pp. 141-156

- Nettesheim, M., 2015. The CJEU's decision on the data retention Directive. In: B. Hess & C. Mariottini, eds. *Protecting privacy in private international and procedural law and by data protection: European and American Developments*. Baden-Baden: Nomos, pp. 57-69
- Newman, A., 2011. Transatlantic flight fights: Multi-level governance, actor entrepreneurship and international anti-terrorism cooperation. *Review of International Political Economy*, 18(4), pp. 481-505
- Nouskalis, G., 2011. Biometrics, e-identity, and the balance between security and privacy: case study of the Passenger Name Record (PNR) system. *The Scientific World Journal*, Volume 11, pp. 474-477
- Öberg, J., 2017. *The legal basis for EU criminal law legislation — A constitutional choice?* Oxford: Hart Publishing
- Ojanen, T., 2014. Privacy is more than just a seven-letter word: The Court of Justice of the European Union sets constitutional limits on mass surveillance. Court of Justice of the European Union, decision of 8 April 2014 in joined cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others. *European Constitutional Law Review*, 10(3), pp. 528-541
- O'Neill, M., 2012. *The evolving EU counter-terrorism legal framework*. Abingdon: Routledge
- Pasquale, F., 2015. *The black box society: The secret algorithms behind money and information*. Cambridge: Harvard University Press
- Pawlak, P., 2009. Network politics in transatlantic homeland security cooperation. *Perspectives on European Politics and Society*, 10(4), pp. 560-581
- Peers, S., 2011. Mission accomplished? EU justice and home affairs law after the Treaty of Lisbon. *Common Market Law Review*, 48(3), pp. 661-693
- Pérez de las Heras, B., 2017. Conclusions. In: B. Pérez de las Heras, ed. *Democratic legitimacy in the European Union and global governance. Building a European demos*. Cham: Palgrave Macmillan, pp. 363-366
- Pérez-Luño Robledo, E., 2019. La nueva normativa Europea para la protección de los datos personales. *Derechos y Libertades*, 40(2), pp. 213-238
- Peyrou, S., 2017. *Accord PNR UE-Canada: Validation par la CJUE du système PNR, des modalités à revoir! (réflexions sur l'avis 1/15 de la CJUE, 26 juillet 2017)*. Available at: <http://www.gdr-elsj.eu/2017/07/28/informations-generales/accord-pnr-ue-canada-validation-cjue-systeme-pnr-modalites-a-revoir-reflexions-lavis-115-de-cjue-26-juillet-2017/> (accessed on 28 May 2020)
- Pfersmann, O., 2002. Contre le néo-réalisme juridique. Pour un débat sur l'interprétation. *Revue Française de Droit Constitutionnel*, 52(4), pp. 789-836
- Piris, J.-C., 2010. *The Lisbon treaty. A legal and political analysis*. Cambridge: Cambridge University Press

Porcedda, M., 2018. On boundaries - Finding the essence of the right to the protection of personal data. In: R. Leenes, R. Van Brakel, S. Gutwirth & P. De Hert, eds. *Data protection and privacy. The internet of bodies*. Oxford: Hart Publishing, pp. 277-312

Research Division of the European Court of Human Rights, 2013. *National security and European case-law*. Strasbourg: Council of Europe

Rizer, A., 2010. Dog fight: Did the international battle over airline Passenger Name Records enable the Christmas-day bomber? *Catholic University Law Review*, 60(1), pp. 77-106

Roberts, A., 2015. Privacy, data retention and domination: Digital Rights Ireland Ltd v Minister for Communications. *Modern Law Review*, 78(3), pp. 535-548

Rosas, A. & Armati, L., 2018. *EU constitutional law. An introduction*. 3rd edition. Oxford: Hart Publishing

Rössler, B., 2005. *The value of privacy*. Cambridge: Polity Press

Rouvroy, A., 2013. The end(s) of critique: Data-behaviourism vs. due-process. In: M. Hildebrandt & E. D. Vries, eds. *Privacy, due process and the computational turn: The philosophy of law meets the philosophy of technology*. New York: Routledge, pp. 143-168

Rouvroy, A. & Berns, T., 2010. Le nouveau pouvoir statistique. Ou quand le contrôle s'exerce sur un réel normé, docile et sans événement car constitué de corps «numériques»... *Multitudes*, 1(40), pp. 88-103

Salminen, J., 2011. Depillarization and the shaping of AFSJ. *Maastricht Journal of European and Comparative Law*, 18(3), pp. 275-302

Saulnier-Cassia, E., 2017. La directive (UE) 2016/681: Miscellanées sur l'utilisation des données des dossiers passagers dans l'Union européenne ou le PNR européen. In: C. Chevallier-Govers, ed. *L'échange des données dans l'Espace de liberté, de sécurité et de justice de l'Union européenne*. Grenoble: Mare & Martin, pp. 207-229

Schermer, B., 2011. The limits of privacy in automated profiling and data mining. *Computer Law & Security Review*, 27(1), pp. 45-52

Scott, J. & Rajamani, L., 2013. Contingent unilateralism — International aviation in the European Emissions Trading Scheme. In: B. Van Vooren, S. Blockmans & J. Wouter, eds. *The EU's role in global governance: The legal dimension*. Oxford: Oxford University Press, pp. 209-223

Servent, A. & MacKenzie, A.,

2011. Is the EP still a data protection champion? The case of SWIFT. *Perspectives on European Politics and Society*, 12(4), pp. 390-406

2017. Eroding Germany's commitment to data protection: Policy entrepreneurs and coalition politics in EU Passenger Name Records. *German Politics*, 26(3), pp. 398-413

Silveira, A. & Freitas, P. M., 2017. Implicações da declaração de invalidade da Diretiva 2006/24 na conservação de dados (“metadados”) nos estados-membros da UE: Uma leitura jusfundamental. *Revista de Direito, Estado e Telecomunicações*, 9(1), pp. 47-68

Spina, A., 2014. Risk regulation of big data: Has the time arrived for a paradigm shift in EU data protection law? Case C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others. *European Journal of Risk Regulation*, 5(2), pp. 248-252

Stoeva, E., 2014. The data retention Directive and the right to privacy. *ERA Forum*, 15(4), pp. 575-592

Stoica, C. & Safta, M., 2015. Theoretical and practical issues relating to the right to the protection of personal data. *Juridical Tribune*, 5(2), pp. 88-105

Tambou, O., 2018. Opinion 1/15 on the EU-Canada Passenger Name Record (PNR) agreement: PNR agreements need to be compatible with EU fundamental rights. *European Foreign Affairs Review*, 23(2), pp. 187-202

Taylor, N., 2014. To find the needle do you need the whole haystack? Global surveillance and principled regulation. *The International Journal of Human Rights*, 18(1), pp. 45-67

Tiberi, G., 2016. La direttiva UE sull’uso dei dati del codice di prenotazione (PNR) nella lotta al terrorismo e ai reati gravi. *Quaderni costituzionali*, Volume 3, pp. 590-593

Tinière, R., 2018. *L’influence croissante de la Charte des Droits Fondamentaux sur la politique extérieure de l’Union Européenne*. Available at: <http://www.revuedlf.com/droit-ue/linfluence-croissante-de-la-charte-des-droits-fondamentaux-sur-la-politique-exterieure-de-lunion-europeenne/> (accessed on 12 May 2020)

Tracol, X., 2014. Legislative genesis and judicial death of a directive: The European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of legal uncertainty about the validity of national laws which enacted it. *Computer Law & Security Review*, 30(6), pp. 736-746

Tridimas, T., 2012. Competence after Lisbon. The elusive search for bright lines. In: D. Ashiagbor, N. Countouris & I. Lianos, eds. *The European Union after the Treaty of Lisbon*. Cambridge: Cambridge University Press, pp. 47-77

Tzanou, M.,

2015. The war against terror and transatlantic information sharing: Spillovers of privacy or spillovers of security? *Utrecht Journal of International and European Law*, 31(80), pp. 87-103

2017. *The fundamental right to data protection. Normative value in the context of counter-terrorism surveillance*. Oxford: Hart Publishing

US Department of Homeland Security, 2010. *U.S.-EU Joint Declaration on Aviation Security*. Available at: <https://www.dhs.gov/news/2010/01/21/us-eu-joint-declaration-aviation-security> (accessed on 8 November 2018)

Vainio, N. & Miettinen, S., 2015. Telecommunications data retention after Digital Rights Ireland: Legislative and judicial reactions in the member states. *International Journal of Law and Information Technology*, 23(3), pp. 290-309

Vedaschi, A.,

2018. The European Court of Justice on the EU-Canada Passenger Name Record Agreement: ECJ, 26 July 2017, Opinion 1/15. *European Constitutional Law Review*, Volume 14, pp. 410-429

2019. Privacy versus security: Regulating data collection and retention in Europe. In: B. Goold & L. Lazarus, eds. *Security and human rights*. 2nd edition. Oxford: Hart Publishing, pp. 275-296

Vedaschi, A. & Graziani, C., 2018. *PNR agreements between fundamental rights and national security: Opinion 1/15*. Available at: <http://europeanlawblog.eu/2018/01/23/pnr-agreements-between-fundamental-rights-and-national-security-opinion-115/> (accessed on 6 November 2018)

Villani, S., 2018. Some further reflections on the Directive (EU) 2016/681 on PNR data in the light of the CJEU Opinion 1/15 of 26 July 2017. *Revista de Derecho Político*, 1(101), pp. 899-928

Von Bogdandy, A. & Schill, S., 2011. Overcoming absolute primacy: Respect for national identity under the Lisbon Treaty. *Common Market Law Review*, 48(5), pp. 1417-1454

Wagner, B., 2019. Liable, but not in control? Ensuring meaningful human agency in automated decision-making systems. *Policy & Internet*, 11(1), pp. 104-122

Walker, N., 2006. In search of the Area of Freedom, Security and Justice: A constitutional odyssey. In: N. Walker, ed. *Europe's Area of Freedom, Security and Justice*. Reprint. Oxford: Oxford University Press, pp. 3-37

Wessel, R. & Blockmans, S., 2012. Between autonomy and dependence: The EU legal order under the influence of international organisations - An introduction. In: R. Wessel & S. Blockmans, eds. *Between autonomy and dependence: The EU legal order under the influence of international organisations*. The Hague: Springer, pp. 1-9

Wilson, K., 2016. Gone with the wind?: The inherent conflict between API/PNR and privacy rights in an increasingly security-conscious world. *Air & Space Law*, 41(3), pp. 229-264

Wolff, S., 2012. Are we ignoring the "risk" in risk based screening? *Aviation Security International*, 18(4), pp. 1-5

Woods, L., 2017. *Transferring personal data outside the EU: Clarification from the ECJ?* Available at: <http://eulawanalysis.blogspot.com/2017/08/transferring-personal-data-outside-eu.html> (accessed on 28 May 2020)

Zalnieriute, M., 2018. Developing a European standard for international data transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement. *The Modern Law Review*, 81(6), pp. 1046-1063