Fundamental Rights European Experts (FREE Group)

Opinion
on the broader and core issues
arising in the PNR Case currently before the CJEU
(Case C-817/19)

by

Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford

November 2021

Final version

Fundamental Rights Europe Experts (FREE Group)

Opinion
on the broader and core issues arising in the PNR Case currently before the CJEU (Case C-817/19)
by Douwe Korff

About the FREE Group:

The Fundamental Rights European Experts Group (FREE Group) is a Belgian non-governmental organisation (*Association Sans But Lucratif*, ASBL), registered at Belgian Moniteur, Number 304811.

According to Articles 3 and 4 of its Statute, the association focus is on monitoring, teaching and advocating in relation to the European Union's Freedom, Security and Justice (FSJ) related policies. In this context, FREE also follows the EU actions in protecting and promoting EU values and fundamental rights in the Member States as required by Articles 2, 6 and 7 of the Treaty on the European Union (risk of violation by a Member State of EU founding values).

https://free-group.eu/free-group-members/

About the author:

Douwe Korff is a Dutch comparative and international lawyer specialising in human rights and data protection. He is emeritus professor of international law at London Metropolitan University and visiting professor at the universities of Zagreb and Rijeka in Croatia; an Associate of the Oxford Martin School of the University of Oxford, a Visiting Fellow at Yale University (Information Society Project), and a Fellow at the Centre for Internet and Human Rights of the European University of Viadrina, Berlin.

Douwe Korff has carried out many studies relating to data protection for the EU, the Council of Europe, the UN (ITU), the British Commonwealth, and the UK authorities.

Acknowledgments:

The author wishes to acknowledge that in preparing this paper he has drawn on the work of other FREE Group members including Emilio de Capitani and Christian Thönnes. He is also grateful for helpful comments from Kristina Irion, co-author of the recent evaluation report on the Dutch PNR Law.

Opinion
on the broader and core issues arising in the PNR Case currently before the CJEU (Case C-817/19)
by Douwe Korff

"Watch lists have a tendency to become blacklists"

"Being subjected to 'further examination' on the basis of a PNR 'hit' is the virtual equivalence to real-world stops and searches"

Fundamental Rights Europe Experts (FREE Group)

Opinion
on the broader and core issues arising in the PNR Case currently before the CJEU (Case C-817/19)
by Douwe Korff

CONTENTS

Attachments:

- o – O – o -

Abbreviations & glossary

Abbreviations:

AIA	Artificial Intelligence Act (proposed)
CFR	(EU) Charter of Fundamental Rights
CJEU	Court of Justice of the European Union ("Luxembourg Court")
DPD	Data Protection Directive (Directive 95/46/EC)
DRD	Data Retention Directive (Directive 2006/24/EC)
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights ("Strasbourg Court")
EAW	European Arrest Warrant
EDPB	European Data Protection Board
EEA	European Economic Area
EU	European Union
GDPR	General Data Protection Regulation
GAO	(US) Government Accountability Office
LED	Law Enforcement Directive
OAS	Organisation of African States
OSCE	Organisation for Security and Cooperation in Europe
PIU	Passenger Information Unit
PNR	Passenger Name Record
PNR Directive	Directive (EU) 2016/681
SIS	Schengen Information System (**SIS II** is the latest version)
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
UN	United Nations
WP29	Article 29 Working Party

For short references to judgments of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights, cited in this opinion, see footnote 53.

Glossary:

Extra-EU flight *	A flight to or from an EU Member State from a third country
Intra-EU flight *	A flight within the EU

* See footnote 96

Analysis data	Data resulting from the analyses of PNR data by the PIUs (acting alone or working with others) including new or improved "pre-determined criteria" or profiles.
PNR data	The data contained in the PNRs
PNR-relevant offences	The offences in relation to which the PNR data are (only) supposed to be used (that must carry a maximum penalty of at least two years imprisonment: see sub-section 4.6).
Not-PNR-relevant offences	Other offences, in particular offences that carry a maximum penalty of less than two years imprisonment
Initial "hit" *	An (almost always) automated match between PNR data as received by the PIUs and any of the databases and lists against which those data are matched by PIU staff.
Confirmed "hit" *	A match that is confirmed by PIU staff after manual review.

* See footnote 66

Formally wanted persons	Persons who have been formally declared under the applicable criminal law or criminal procedure law to be suspected of involvement in a crime, formally wanted for a crime, formally charged with a crime, prosecuted for a crime, or convicted of a crime.
Persons of interest	Persons who the law enforcement or intelligence agencies have earmarked as being of interest, but who are not (yet) formally wanted persons.
Article 36 alert	An alert entered into the SIS database requiring authorities to carry out "discreet checks, inquiry checks or specific checks" on the person to whom the alert is linked (see sub-section 2.3)

- o – O – o -

Opinion
on the broader and core issues arising in the PNR Case currently before the CJEU (Case C-817/19)
by Douwe Korff

1. Introduction

In April 2016, the EU adopted a directive on the mandatory provision of so-called passenger name records (PNR) by airlines to the EU Member States (hereafter "the PNR Directive" or simply "the directive").[1] The directive, being a directive, had to be transposed into national law of the Member States, and this was duly done, *inter alia* in Belgium, by means of the Law of 25 December 2016 "on the processing of passenger data". The directive and the national laws were contentious and denounced by many human rights and digital rights groups as enabling undue mass surveillance.

One of these groups, the Belgian NGO *Ligue des Droits Humain*, challenged the directive and the Belgian law in the Belgian Constitutional Court and on 17 October 2019 the Constitutional Court agreed to a request for a preliminary ruling to the Court of Justice of the European Union (CJEU).[2] The request was lodged with the CJEU on 31 October 2019.[3] The reference contained ten preliminary questions on the interpretation of the PNR Directive and its compatibility with EU primary law.

13 July 2021, an oral hearing was held at the CJEU where a series of elements of the directive were discussed.[4] The hearing involved participants representing:

- the applicant, the *Ligue des Droits Humains*;
- the European Parliament, the European Council, and the European Commission; and
- the governments of Belgium, the Czech Republic, Latvia, Germany, Estonia, Ireland, Spain, France, Cyprus, the Netherlands, and Poland.

The judge-rapporteur, Mr. von Danwitz, asked a series of questions that turned on four issues:

1. the reliability, respectively fallibility, of the system – i.e., of the proposed singling out of individuals from the PNR data - and whether the system can be said to be "necessary" for that purpose;
2. the level of severity of the interference with fundamental rights resulting from the system;
3. the issue of discrimination, in particular of indirect discrimination, that may result from the system; and
4. (in the light of the above) the proportionality of the system.

---

1 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 L 119, 4 May 2016, pp. 132 – 149, available at: https://eur-lex.europa.eu/eli/dir/2016/681/oj

2 Arrest n° 135/2019 of 17 October 2019.

3 Case C-817/19: Request for a preliminary ruling from the Cour constitutionnelle (Belgium) lodged on 31 October 2019 — Ligue des droits humains v Conseil des ministers, OJ C 36, 3.2.2020, p. 16–17, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62019CN0817

4 See Christian Thönnes, *On Flights, Rock Concerts and the Needle in a Haystack A report from the Court of Justice of the European Union's oral hearing on the PNR directive*, EU Law Analysis blog, 17 September 2021, available at: https://eulawanalysis.blogspot.com/2021/09/on-flights-rock-concerts-and-needle-in.html

However, as I will show in this opinion, some issues were not fully addressed, and on some other issues – in particular, the question of "false positives" and the "base-rate fallacy" – the participants appeared to not fully understand the statistics or mathematics.

In this opinion, I will try to place the PNR Directive and the processing of personal data that is intended, or allowed and envisaged, under the directive in their wider contexts (section 2, below) and adduce the relevant legal standards that are to be applied to the processing (as elaborated in the case-law of the CJEU in particular) (section 3).

In section 4, I analyse the PNR Directive in some detail, with reference to various aspects of the directive (aims, legal bases, competent authorities, "PNR-relevant offences", categories of data and categories of data subjects, etc.), before focussing on the various forms of data matching that are carried out, or to be carried out, under the directive (see section 4, sub-section 4.9) and on the access to the data and the dissemination and subsequent use of the data (sub-sections 4.10 and 4.11). I also discuss the consequences of a "match" in the various kinds of data matching (sub-section 4.12).

In section 5, I note the inexcusable lack of serious data on the use of the PNR data and on the implications of this use (sub-section 5.1), before making an attempt at an assessment of the PNR Directive and the processing of personal data under it, in particular in terms of the suitability, effectiveness and proportionality of the processing in relation to the stated aim of the directive: the prevention, detection, investigation and prosecution of terrorist offences and serious crime (section 5.2). In section 5, sub-section 5.3, I set out my overall conclusions.

A number of attachments expand on certain relevant matters.

An Executive Summary is provided separately, together with a one-page "at a glance" overview of my findings and conclusions.

In writing this opinion, my main sources have been the European Commission's review report on the implementation of the directive and the staff working document that accompanied that review report.[5] I also draw extensively on the report on the evaluation of the Dutch PNR Law, carried out by Dutch researchers Kristina Irion and Romy van Es at the request of the research and documentation centre (WODC) of the Dutch Ministry of Justice and Security.[6]

- o – O – o -

[5] Respectively:
- 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 July 2020 (hereafter: "**Commission report**"), available at: https://op.europa.eu/en/publication-detail/-/publication/4bfd0de3-cda3-11ea-adf7-01aa75ed71a1/language-en
- Commission Staff Working Document accompanying the above Commission Report, SWD(2020) 128 final, 24 July 2020 (hereafter: "**Staff working document**"), available at: https://op.europa.eu/en/publication-detail/-/publication/9c419b94-cda3-11ea-adf7-01aa75ed71a1/language-en/format-PDF/source-search

[6] Irion, K., Es, R. van, Meeren, K. van der, & Dijkman, D, Evaluatie PNR-Wet (hereafter: "**Evaluation of the Dutch PNR Law**"), WODC rapport 3181, October 2021, available at:
http://hdl.handle.net/20.500.12832/3118
https://www.eerstekamer.nl/overig/20211112/evaluatie_pnr_wet_wodc_oktober/document

2. PNR in context

2.1 The early trend

Early in the current century, Ian Brown and I noted that, in particular in relation to terrorism (and especially after "9/11"), policing was moving from finding perpetrators of crimes that had been committed and persons who posed an immediate danger, to "pro-actively" "identifying"[7] individuals who "*may be*" involved (or even more tentatively, who could possibly or probably *become* involved) in terrorism; that in this activity the roles of the national intelligence agencies and the law enforcement agencies were becoming increasingly intertwined, with the latter adopting sophisticated (but often inherently flawed) "risk assessment" and "analysis" methodologies initially developed by the former; and that this trend was spreading to other law enforcement areas such as "serious crime". We concluded that:[8]

> Policing in the early-21st century increasingly extends beyond the traditional police tasks of investigation and prosecution of crime and the countering of immediate threats, to "preventive" action against suspected criminals, and indeed against not-necessarily-unlawful actions which are nevertheless deemed to be socially unacceptable or indicative of possible future illegality. At the same time, **policing (for all these ends) has become more sophisticated, more intrusive, more centralised, and more secret, than ever since the Second World War**. And the trend is towards yet greater merging of police work with other State activities aimed at ensuring comprehensive social control, yet more sophistication, yet more intrusion, yet more central governmental (and intergovernmental) control, and yet greater secrecy.

Even then, we already linked the issue of big data datamining to the processing of airline passenger data.[9]

Privacy International showed that **in the EU this trend was actively supported as a strategy**, the aim of which was (and is):[10]

> **to facilitate targeted searches for would-be terrorists** (...). It is closely connected to the German initiative on computer-aided preventive searches carried out by individual

---

[7] I discuss the ambiguous meaning of the word "identify" in this context in the introduction to section 4.9, below.

[8] Ian Brown & Douwe Korff, Privacy and Law Enforcement, study for the UK Information Commissioner, released on the Commissioner's website in September 2004 as "*Striking the Right Balance: Respecting the Privacy of Individuals and Protecting the Public from Crime*", Paper No. 4, *The legal framework: an analysis of the 'constitutional' European approach to issues of data protection and law enforcement*, p. 146 (repeated on p. 164), emphasis added. No longer available from the ICO website but available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3737428

[9] *Idem*, Paper No. 3, *TIA & PNR* (referring to the US project *Total Information Awareness* and Passenger Name Records, and the links between them), at pp. 47 – 86.

[10] Privacy International, Report on Discrimination and Anti-Terror Policy Across Europe, December 2005, still available at the Internet Archive, at: https://web.archive.org/web/20171019104526/https://www.privacyinternational.org/sites/default/files/Discrimination%20and%20Anti-Terror%20Policy%20Across%20Europe_1.pdf
I will address the still pertinent issue of discrimination in this context in section 4, sub-section 4.9(fe), at (ii).

> Member States on the basis of coordinated **offender profiles** (Europewide electronic profile searches). Such searches are essential to the success of security service operations. (...)
>
> On the basis of this profile each Member State searches the relevant national data bases (e.g. registers of residents, registers of foreigners, universities etc.) subject to the provisions of national law, for persons who need to be vetted more closely by the security authorities. The more detailed the offender profile, the smaller the group of persons covered by the search.[11] (emphasis added)

Thus, terrorist profiling was already under discussion long before the adoption of the PNR Directive. The relevant profiles were defined as early as 2002 by the EU Council, as follows:[12]

> **Developing terrorist profiles means putting together a set of physical, psychological or behavioural variables, which have been identified, as typical of persons involved in terrorist activities and which may have some predictive value in that respect.**

At the time, the envisaged profiles were to be based on a long (but still open-ended) list of issues (data elements) that were deemed relevant:[13]

> The following might be included as elements in developing terrorist profiles:
>
> - nationality,
> - travel document,
> - method and means of travel,
> - age,
> - sex,
> - physical distinguishing features (e.g. battle scars),
> - education,
> - choice of cover identity,
> - use of techniques to prevent discovery or counter questioning,
> - places of stay,
> - methods of communication,
> - place of birth
> - psycho-sociological features,
> - family situation,
> - expertise in advanced technologies,
> - skills at using non-conventional weapons (CBRN),
> - attendance at training courses in paramilitary, flying and other specialist techniques.

---

[11] Council of the European Union, Memo from German Delegation to the Article 36 Committee, Subject: Note on computer-aided preventive searches carried out by individual Member States on the basis of coordinated offender profiles (Europe-wide electronic profile searches), Brussels, October 31, 2002, 13626/02, LIMITE ENFOPOL 130. [original footnote]
This fed into a more formal EU policy, reflected in a Council Recommendation on the development of terrorist profiles. The draft recommendation (since endorsed by COREPER) dated 18 November 2002 (Council Document 11858/3/02REV3 LIMITE ENDOPOL 117) is available at:
https://data.consilium.europa.eu/doc/document/ST%2011858%202002%20REV%203/EN/pdf

[12] Council of the European Union, Council Recommendation on the development of terrorist profiles (previous footnote), Annex A, *Best practice*.

[13] *Idem*.

Several of the above-mentioned elements were (and are) problematic. For instance, what is covered by the element of "education"? The name of a school or university can be a proxy for religious beliefs. A girl who attended a Northern Ireland school named after the Virgin Mary is almost as certain to be Roman Catholic as a boy from the Province who attended a King William school is a protestant. It is unclear whether, under this heading, records were to be kept of individuals who attended Wahabi-inspired madrassas in Pakistan. Or whether all former pupils of all such religious schools should automatically be labelled "suspicious". In relation to "methods of communication" similar questions arose (and arise): are all individuals who use end-to-end encrypted messaging automatically suspect? *Re* "family situation": are the fathers, brothers, sisters, wives, sons and daughters of "known" terrorists all automatically deemed "suspects" (or "possible suspects" or "persons of interest")?[14] What was meant by "psycho-sociological features"? Breakdowns? Poverty? Would the data on an individual have to meet a certain number of these elements to be regarded as matching a profile? If so, how many? Were the elements weighted? None of this was made clear, even at the time.

As further discussed in section 4, sub-section 4.9(a) – (e), below, the information provided in relation to the operation of the PNR Directive also still, for now, appears to focus on specific elements, both relatively "hard" ones such as name, date of birth, nationality, etc., and "soft" ones such as "suspicious" travel agents, "suspicious" travel routes, "suspicious" amounts of luggage, etc. In relation to those, similar questions arise (as discussed in those sections). However, as discussed in sub-section 4.9(f), the PNR Directive also clearly allows for, and is intended to be used for, more complex assessments – in line with the trend noted next.

2.2 The "mining" of bulk data sets

One more recent element of the EU strategy is **the facilitating of bulk access by law enforcement and national intelligence agencies to large-scale databases and data sets held by the private sector on whole – of course, overwhelmingly innocent – populations** (what I will call "mass surveillance").[15] The data sets to which law enforcement and intelligence agencies (working increasingly closely together: see above) want access in bulk include data on electronic communications (both on the actual communications and "metadata"), financial data – and data on people travelling to and in the EU, in particular air passengers.

The two most egregious examples of this facilitating of access to bulk data are the introduction of the Data Retention Directive (since invalidated by the Court of Justice: see sub-sections 2.4 and 3.1, below) and the PNR Directive.

Crucially, the access to bulk data is used not only to find "known" terrorists and serious criminals by trying to match the data on those "known" individuals to data in those data sets, but increasingly also to try and detect "hidden" patterns and "identify" previously "unknown"

[14] On the category of "persons of interest", see section 4, sub-section 4.7, below.

[15] On my use of this term, see Box 1 on page 13.

(probably or possibly) bad people.[16] This constitutes a paradigm shift. As Marie Georges and I pointed out six years ago with specific reference to PNR data:[17]

> In a world of massive "Big Data**", innumerable elements can be factored in, and links can be established between factors that no-one would have thought were linked in advance**:[18]
>
> > "**Big data is not just about lots of data, it is about having the ability to extract meaning; to sort through the masses of data elements to discover the hidden pattern, the unexpected correlation.**"

This **mass surveillance** is carried out by means of **increasingly sophisticated, Artificial Intelligence (AI) based algorithms** (as rightly criticised by civil society, as noted below, at 2.4).

These more sophisticated algorithms are supposed to have more "predictive value" than the more primitive profiles of two decades ago – but in fact also suffer from serious limitations, as I will discuss in section 4, sub-section 4.9(fe), below).

In 2013, Edward Snowden revealed the scope and depth of the processes and technologies involved, as practised by the US intelligence agencies (working closely with the UK agencies) – but which we now know are also carried out by EU Member States, and encouraged by the EU.[19] Europol in particular plays an ever-increasing role in this respect: see below, at 2.3.

---

[16] See Douwe Korff, Protecting the right to privacy in the fight against terrorism, "*Issue Paper*" written for the Commissioner for Human Rights of the Council of Europe, December 2008, available at: https://wcd.coe.int/ViewDoc.jsp?Ref=CommDH/IssuePaper(2008)3&Language=all

[17] Douwe Korff & Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards, pp. 23 – 24, emphases added, report prepared for the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) of the Council of Europe, June 2015, available at: https://rm.coe.int/16806a601b

[18] The quote is from Art Coviello, executive chairman of RSA, the security division of EMC, see: http://www.computerweekly.com/news/2240178641/Embrace-big-data-to-enable-better-security-says-RSA (emphasis added) [original footnote]

[19] All the documents leaked by former NSA contractor Edward Snowden that have subsequently been published by news media are available at The Snowden Archive, maintained by Canadian Journalists for Free Expression, at: https://www.cjfe.org/snowden

For reports on the revelations re the USA and information on EU Member States' activities, see:

- European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE), Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (rapporteur Claude Moraes), EP Document A7-0139/2014, 21 February 2014, available at; https://www.europarl.europa.eu/doceo/document/A-7-2014-0139_EN.html
- Parliamentary Assembly of the Council of Europe (PACE), Report on Mass Surveillance (rapporteur: Pieter Omtzigt), PACE Document 13734, 18 March 2015, available at: https://ccdcoe.org/uploads/2018/11/CoE-150318-MassSurveillanceReport.pdf

For an overview of national laws and practices, see also:

- Douwe Korff, Ben Wagner, Julia Powles, Renata Avila and Ulf Buermeyer, Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes, comparative report covering Colombia, DR Congo, Egypt, France, Germany, India, Kenya, Myanmar, Pakistan, Russia, South Africa, Turkey, UK, USA, prepared for the World Wide Web Foundation, January 2017, available at: https://ssrn.com/abstract=2894490

Here, it must suffice to note that, **in the footsteps of the US and UK intelligence services (as revealed by Snowden), the EU Member States' law enforcement agencies are also increasingly using their access to bulk data – bulk e-communications data, financial data, PNR data, etc. – to "mine" the big data sets by means of sophisticated, self-learning algorithms and Artificial Intelligence (AI). The PNR Directive must be assessed also and especially in the light of this increasing, dangerous trend.**

BOX 1:

Whether the processing discussed in this opinion constitutes "mass surveillance".

As Eric King pointed out in his 2019 report with Greg Nojeim on UK surveillance practices for the Center for Democracy and Technology:[20]

"*There are a number of different terms to describe [the relevant] collection practices, each with contested definitions. Terms like mass surveillance, bulk collection, and targeted or untargeted interception all have different meanings to different stakeholders in different countries, and there isn't yet a common lexicon.*"

He used the terms "bulk collection" and "bulk interception" interchangeably, following this loose definition provided by the US National Academy of Sciences:

"*If a significant portion of the data collected is not associated with current targets, it is bulk collection; otherwise, it is targeted. There is no precise definition of bulk collection, but rather a continuum, with no bright line separating bulk from targeted. The committee acknowledges that use of the word 'significant' makes its definition imprecise as well.*"

In its judgment in *Digital Rights Ireland*, the Court of Justice of the EU referred to this as:

"*[processing] in a generalised manner of large data sets*" (in that case, of data on all persons who use electronic communications and all means of electronic communication as well as all communications traffic [meta] data) *"without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime*" (para. 57).

In this opinion, I use the terms "bulk collection" and "mass surveillance" interchangeably because "bulk collection" as defined above and "generalised processing" as described by the CJEU, in my view *ipso facto* constitutes mass surveillance.

2.3 The Schengen Information System (SIS), Europol and European Arrest Warrants (EAWs)

The PNR data processed under the PNR Directive by the special Passenger Information Units (PIUs) of the EU Member States (discussed in section 4) are regularly checked against the data and "alerts" in the Schengen Information System (SIS, more specifically SIS II),[21] and those

[20] Center for Democracy & Technology (CDT), Not a Secret: bulk interception practices of intelligence agencies, September 2019, available at: https://cdt.org/insights/not-a-secret-bulk-interception-practices-of-intelligence-agencies/

[21] Established by Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 205, 7 August 2007, pp. 63 – 84, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32007D0533

data, and the results of the "analyses" of these data, can also be shared (under certain circumstances) with Europol (as discussed in section 4, sub-section at 4.11(b), below).

This is not the place to discuss SIS, EAWs or Europol in any detail. However, three matters should be noted. First of all, SIS allows for searches, not only for persons who are not entitled to enter into or stay in the Schengen Area; persons for whom a European Arrest Warrant has been issued; missing persons, including children; persons sought to assist with a criminal judicial procedure (such as witnesses); and objects sought in relation to criminal proceedings (such as vehicles, travel documents, credit cards, number plates and industrial equipment); - but also for "**persons and objects for discreet checks, inquiry checks or specific checks**".[22] This last type of alerts (an "Article 36 alert") may be issued against individuals who are not yet convicted of, or charged with, any offence (more specifically, one of the offences to which the European Arrest Warrant applies, as listed in Article 2(1) and (2) of Framework Decision 2002/584/JHA):

- where there is a clear indication that a person intends to commit or is committing such a crime [an EAW-relevant crime]; or
- where an overall assessment of a person, in particular on the basis of past criminal offences, gives reason to believe that that person may also commit such a crime in the future.

(Article 36(2)(a) and (c))

The formal requirement of Article 36(2)(a) that "*there is **a clear indication** that a person intends to commit or is committing [a relevant] crime*" appears to come close to the requirement for formally declaring a person to be a suspect under criminal or criminal procedure law. However, it is clear that **actually such alerts are specifically aimed at persons who are not (yet) – and cannot (yet) – formally be declared a suspect under criminal or criminal procedure law**, i.e., against whom there is as yet no real evidence that they will commit a relevant crime. This also applies to the other condition, under Article 36(2)(c), that there must be "***reason to believe***" that a person may re-offend.[23]

---

[22] The category of "inquiry checks" was added in 2016 in 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) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, OJ L 312, 7.12.2018, p. 56–106, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1862
As explained in the proposal for this change:
"*Article 37 introduces a new form of check, the 'inquiry check'. This is, in particular, intended to support measures to counter terrorism and serious crime. It allows authorities to stop and question the person concerned. It is more in-depth than the existing discreet check, but does not involve searching the person and does not amount to arresting him or her. It may, however, provide sufficient information to decide on further action to be taken.*"

[23] The various levels of suspicion and factual underpinning of suspicion in different phases of the criminal justice process are elaborated in more detail in some jurisdictions than in others. For instance, German law distinguishes between "initial suspicion" (*Anfangsverdacht*) and "concrete suspicion" (read: suspicion based on "concrete" facts, rather than vague indications and mere subjective assessments, *konkrete Tatverdacht*), etc. Although some of the terminology in the regulation appears to come close to the latter German concept, it is not clear whether the same, relatively strict tests apply – or more pertinently: are applied by the Member States (indeed, even by Germany)– in relation to SIS alerts from intelligence agencies.

In addition:

> **an alert may be issued in accordance with national law, at the request of the authorities responsible for national security**, where there is **a concrete indication** that the information referred to in Article 37(1) is necessary in order to prevent a serious threat by the person concerned or other serious threats to internal or external national security.
>
> (Article 36(3), emphasis added)

This provision is rather muddled. It does not actually say that there must be a "concrete indication" that a specific person poses a "serious threat" of the kind mentioned. However, presumably that is nevertheless how the provision should be read, i.e., that in order for a person to be made subject to an intelligence agency alert under Article 36(3) there must be **some "concrete indication" that that person poses a serious threat**, and **the information listed in Article 37(1) must be "necessary" to prevent that threat**.[24]

The information in question includes matters such as:

- the location of specific persons and objects, with the relevant date and time;
- routes travelled;
- persons accompanying the subject of the alert or the occupants of the vehicle, boat or aircraft
- identity and travel document details;
- details of payment methods used;
- etc.

These categories of data are indeed to be found in the PNR data sets.

However, it is not clear who checks the quality of the "concrete indications" that the agencies may rely on; this appears to be largely left to the agencies themselves (or to the other agencies through which they issue alerts).[25]

In practice, "Article 36 alerts" – be they issued by law enforcement agencies under paragraph 2 of that article or by intelligence agencies under paragraph 3 – relate to what are generally referred to – also explicitly in the Commission staff working document on the operation of the PNR Directive, extensively referenced in section 4, below – as "persons of interest", against whom there will often be little substantial "concrete" evidence such as would be required to formally declare them to be a suspect, let alone to arrest, charge, indict or convict them of any criminal offence. I discuss this category of persons further in section 4, sub-section 4.7, below.

[24] As the language of Article 36(3) indicates, the intelligence agencies do not enter alerts into SIS themselves, directly, but rather, must ask relevant other authorities (law enforcement authorities or a ministry) to issue an alert on their behalf, "in accordance with national law".

[25] See the previous footnote.

There has been concern (albeit only expressed in cautious terms in published documents) about the fact that **"Article 36 alerts" have been increasing**.[26] The SIS II Supervision Coordination Group (SIS II SCG)'s Activity Report for 2018 – 2019 (the latest available) mentions the following as one of its two "main activities" in that period:[27]

> **Article 36 alerts**
>
> In view of the increase of alerts entered in the SIS II based on Article 36 of the SIS II Decision (i.e. data on persons or vehicles, boats, aircrafts and containers entered for the purposes of discreet checks or specific checks), the Group decided to carry out a joint exercise on this issue.
>
> The Group elaborated a checklist to serve as a guide for DPAs when conducting national investigations on the use of these alerts. The purpose of these inspections is to enable DPAs to conduct an overall assessment of the level of compliance with the legal basis and to report such results with possible recommendations.

I have not been able to find further information on this "joint exercise", or on the "checklist" or the "inspections".

However, it is highly notable – and in my opinion deeply worrying – that **the evaluation of the operation of the Dutch PNR law found that in 2020 in that EU Member State, 82.4% of all confirmed "hits" against the Schengen Information System were "hits" against "Article 36 alerts", i.e., against "persons of interest" who were not (yet) formally wanted under the criminal law** (i.e., not yet formally declared to be a suspect, or charged, indicted or convicted under criminal or criminal procedure law).[28]

Secondly, the crimes in question must carry a custodial sentence of a maximum period of at least 12 months – which covers a wide range of offences, not all of them necessarily very serious. This range of offences is also much wider than the range of offences in relation to which PNR data can be processed ("PNR-relevant offences") – an issue I will discuss further in section 4, sub-sections 4.6 and 4.9, below.

And third, again controversially, the European Union Agency for Law Enforcement Cooperation, Europol, has become increasingly involved in algorithm/AI-based data analysis (or at least in the research underpinning those technologies):[29]

---

[26] See Summary of the discussions at the SIS II Supervision Coordination Group's 11th meeting in Brussels on 12 June 2018, available at: https://edps.europa.eu/sites/default/files/publication/18-06-12_summary_of_meeting_sis_ii_scg_en.pdf

[27] SIS II Supervision Coordination Group Activity Report 2018-2019, p. 8, available at: https://edps.europa.eu/system/files/2021-02/sis_activity_report_2018-2019_en.pdf

[28] Evaluation of the operation of the Dutch PNR law (footnote 6, above), p. 6.

[29] Niovi Vavoula and Valsamis Mitsilegas, Strengthening Europol's mandate: A legal assessment of the Commission's proposal to amend the Europol Regulation, study requested by the European Parliament's Civil Liberties (LIBE) Committee, May 2021, p. 12, emphasis added, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694200/IPOL_STU(2021)694200_EN.pdf

> Europol is [already – DK] described as the EU's 'criminal information hub'[30] and the main 'information broker',[31] as it facilitates information exchange between EU Member States, Europol, other EU bodies, international organisations and third countries, and produces criminal intelligence on the basis of information acquired from various sources, including Member States and its partners. **Amongst its many tasks, Europol** also supports and coordinates cooperation on cross-border police work and **produces** regular assessments that offer comprehensive, **forward-looking analyses of crime and terrorism in the EU**.

Europol is specifically also involved in such matters in relation to PNR:[32]

> The use of pre-determined criteria – more demanding from the operational, analytical and technical point of view – is still at an early stage of implementation in some Member States. **Since January 2020, Europol provides assistance to the Member States in the development of this processing method through its Travel Intelligence Task Force.** The Task Force centralises, analyses and distributes relevant information and intelligence on patterns, trends and modus operandi which can be used by the Member States' Passenger Information Units to develop targeted, proportionate and specific targeting rules. Training on the development of pre-determined criteria is also supported through an ongoing EU-funded project, financed under the ISF-Police Union Actions.[33]

---

30 'Europol Strategy 2020+' (*Europol*, 5 February 2019) < https://www.europol.europa.eu/publications-documents/europolstrategy-2020 > accessed 3 May 2021, 4 [original footnote]

31 Thomas Wahl, 'The European Union as an Actor in the Fight Against Terrorism' in Marianne Wade and Almir Maljevic (eds), A War on Terror? (Springer 2010) 144. [original footnote]

32 Commission Staff working document (footnote 5, above), section 3.5, on p. 8, emphasis added.

33 A footnote refers to section 3.1 of the document for further information. There, it is explained that:
"The Commission has supported the Member States throughout the whole implementation process by coordinating regular meetings, facilitating the exchange of best practice and peer-to-peer support, and providing financial assistance.
In particular, to support the implementation of the PNR Directive, the Budgetary Authority reinforced the 2017 Union budget with EUR 70 million for the Internal Security Fund-Police (ISF-Police), specifically for PNR-related actions. The Commission has also funded four PNR-related projects under the Union Actions of the ISF-Police. These projects aimed to ensure that the Passenger Information Units of the Member States developed the capabilities needed to exchange PNR data or the results of processing such data with each other and with Europol.
The first of these projects was the 'Pilot programme for data exchange of the Passenger Information Units', or 'PNRDEP'. The project, coordinated by Hungary and implemented from February 2016 to June 2017, was awarded EUR 1.15 million to look into the possibilities **facilitating the exchange of PNR data between the Passenger Information Units and Europol**. It was followed by the PIU.net project, which was coordinated by the Netherlands and implemented from November 2017 to September 2019, with a grant of EUR 3.78 million. Its objective was to deliver a technical solution that would facilitate the exchange of PNR data between the Passenger Information Units. A third project, led by Hungary under a EUR 855,000 grant (currently ongoing), focuses on developing and providing training for PNR practitioners in the Member States. In addition, Germany is currently coordinating a project that focuses on exploring the means **to enhance the interoperability of PNR data with IT systems of law enforcement authorities at both national and EU level**, with a budget of EUR 2.61 million.
These funding measures are in addition to the grants awarded under the Call for Proposals PNR 2012 within the Specific Programme for Prevention of and Fight against Crime (ISEC) 2007-2013, which overall amounted to EUR 37 million 29 and aimed to help implement national schemes based on domestic PNR legislation adopted prior to the adoption of the PNR Directive." (pp. 5 – 6, emphases added)

Last year the Commission proposed to further expand this role by *inter alia*:[34]

- enabling Europol to receive personal data (including bulk data) directly from private parties on a more regular basis, inform such private parties of missing information, and ask Member States to request private parties to share further information;
- enabling Europol to process large and complex datasets and to carry out "pre-analyses" of those large and complex datasets; and
- strengthening Europol's role on research and innovation, aimed at the development of tools, including the use of AI for law enforcement, and involving the development of new technologies for which extensive processing of large quantities of personal data may be required, e.g., to create and test algorithms or for encryption;

As EDRi put it:[35]

> the proposal suggests that Europol should play a bigger role in developing and shaping future policing technologies that will be deployed in Europe in the coming years. For that, the Agency would help set the priorities in terms of EU funding for research projects in the field of security and train and test itself algorithms to develop tools for EU law enforcement authorities.

In the next sub-section, I note the strong criticisms by EDRi and dozens of other NGOs of the trends described in this and the previous sub-sections. I discuss algorithm/AI-based data mining and profiling further in section 3, sub-section 4.9(f), below.

2.4 Criticism

Various EU instruments that compel private entities to collect and/or retain personal data on whole populations (or large sections of whole populations such as all air passengers) in order to facilitate bulk access to the very large data sets for law enforcement and national security purposes have been strongly criticised and challenged by civil society and human rights experts over many years, including specifically in relation to the bulk collection of PNR data. Here, it will suffice to provide a few short extracts from EDRi's overview of the criticisms and challenges (that focusses on mandatory retention of e-communications data but is equally relevant to the mandatory collection and making available of PNR data):[36]

---

[34] European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation, COM(2020) 796 final (Europol proposal of 2020), available at: https://beta.op.europa.eu/en/publication-detail/-/publication/0d3eb9fd-3b02-11eb-b27b-01aa75ed71a1/language-en/format-PDF/source-search
In my brief indents, I draw on the LIBE study, referenced in footnote 29, above.

[35] EDRi, Recommendations on the revision of Europol's mandate, position paper on the European Commission's proposal amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation, 10 June 2021, pp. 3 – 4, available at: https://edri.org/wp-content/uploads/2021/06/Recommendations-on-the-revision-of-Europols-mandate.pdf

[36] EDRi, *Europe's Data Retention Saga and its Risks for Digital Rights*, 2 August 2021, available at: https://edri.org/our-work/europes-data-retention-saga-and-its-risks-for-digital-rights/

> In 2014, the CJEU brought down the Data Retention Directive[37] in the *Digital Rights Ireland* decision[38] for its incompatibility with the EU Charter of Fundamental Rights. That Directive had required providers of electronic communications services to retain metadata about its customers' communications, i.e. data ("communications data") that identify the "who", "where" and "when" of those communications rather than their content. …
>
> The 2014 decision concerned two cases (later merged by the court) brought by EDRi's members *Digital Rights Ireland* and a large number of complainants organised by Austrian organisation *AK Vorrat* (now called *epicenter.works*). The court's reasoning set out in this ruling was confirmed and reinforced in *Tele2/Watson* two years later, when the court held again that any indiscriminate data retention obligation on telecommunications providers was unjustified in a democratic society.[39] …
>
> Unfortunately, this was not the end of the story. In contempt of these two very clear judgments, several EU Member States decided to wilfully ignore the Court and persisted in implementing or creating new national data retention legislation. In most cases, they argued that their respective national regime was, in fact, compliant because it was either "restricted" in some sense or outside of EU competence and thus the Court's jurisdictional remits.
>
> In practice, however, those claims were false, as demonstrated by *Privacy International* in its 2017 report, which showed that those laws were actually still general and indiscriminate.[40] …
>
> Despite EDRi's repeated calls, the Commission refused to launch a single infringement procedure against (likely) infringing Member States. Instead, it promised to "monitor" national data retention laws, meaning individuals had to rely on civil society organisations and other stakeholders to protect their rights and challenge mass surveillance laws in different Member States, such as France, Belgium, Ireland, Austria, Sweden, Germany, etc (as summarised in EDRi's latest report on data retention).[41]

(slightly edited, footnote references added). PNR data are covered in the broader EDRi booklet referenced in footnote 41, below.

37 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 April 2006, pp. 54–63, available at: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32006L0024

38 CJEU (Grand Chamber) judgment of 8 April 2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238, available at: https://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN

39 CJEU (Grand Chamber) judgment of 21 December 2016 in Joined Cases C-203/15 and C-698/15, *Tele2/Watson*, ECLI:EU:C:2016:970, available at: https://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=EN

40 Privacy International, A Concerning State of Play for the Right to Privacy in Europe: National Data Retention Laws since the CJEU's Tele-2/Watson Judgment, September 2017, available at: https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf

41 EDRi, Data Retention Revisited, September 2020, available at: https://edri.org/wp-content/uploads/2020/09/Data_Retention_Revisited_Booklet.pdf

> Meanwhile, at the EU level, the Council continued to explore all possible options to keep, and even expand, current data retention schemes, notably by creating a dedicated expert working group. …
>
> More recently, the CJEU was asked a third time to confirm its position and strongly incentivised to water down existing protections. The Court at least partially relented in 2020 in three connected cases brought by *Privacy International*[42] and by *La Quadrature du Net* and *Ordre des barreaux francophones et germanophone* and others.[43]
>
> In its decision in *La Quadrature du Net*, the Court introduced an exception to the "general and indiscriminate data retention" prohibition where there is a genuine and present or foreseeable serious threat to national security, justifying the enactment of a state of emergency in a Member State. Moreover, the Court gave in to the possibility of preventively retaining all IP addresses to tackle serious crime, public and national security, despite this measure being considered a serious interference with fundamental rights.
>
> Even with these concessions, the Belgian, French and British laws were deemed illegal and needed to be expressly changed or repealed. …
>
> Nevertheless, while acknowledging this non-compliance, the European Commission confirmed in a European Parliament's hearing that it does not plan to act on it, referring to the "dynamic of a cooperative spirit with all Member States" as justification of its lack of political courage. That "cooperative spirit" also saw the Commission consulting with the Member States about the way forward and exploring possible approaches and solutions for responding to law enforcement and judiciary needs in line with the Court's case law.

I summarise the case-law of the Court of Justice of the EU and of the European Court of Human Rights on bulk data surveillance in the next section.

Before that, I should still first notice the strong criticisms by civil society of the increasing use of AI. These are neatly summarised in an Open Letter, coordinated by EDRi and its members, calling for regulatory limits on deployments of artificial intelligence that unduly restrict human rights, co-signed also by dozens of other NGOS including *Amnesty International*, *Human Rights Watch*, *Liberty* and the *Ligue des Droits Humains*. These are the paragraphs most directly relevant to the use of PNR data in AI-based data mining:[44]

---

[42] CJEU (Grand Chamber) judgment of 6 October 2020 in Case C-623/17, *Privacy International*, ECLI:EU:C:2020:790, available at: https://curia.europa.eu/juris/document/document.jsf?docid=232083&doclang=EN

[43] CJEU (Grand Chamber) judgment of 6 October 2020 in Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature Du Net* (*LQDN*), *Ordre des barreaux francophones et germanophone* and others, ECLI:EU:C:2020:791, available at: https://curia.europa.eu/juris/document/document.jsf?docid=232084&doclang=EN

[44] EDRi *et al*, Open letter: Civil society call for the introduction of red lines in the upcoming European Commission proposal on Artificial Intelligence, 12 January 2021, paras. 2 and 4, embedded links replaced by footnotes, original emphases, available at: https://edri.org/wp-content/uploads/2021/01/EDRi-open-letter-AI-red-lines.pdf

Uses of AI at the border and in migration control:

The increasing examples of AI deployment in the field of migration control pose a growing threat to the fundamental rights of migrants, to EU law, and to human dignity. Among other worrying use cases, AI has been tested to purportedly detect lies[45] for the purposes of immigration applications at European borders and to monitor deception in English language tests through voice analysis[46], all of which lack credible scientific basis. In addition, EU migration policies[47] are increasingly underpinned by AI systems, such as facial recognition, algorithmic profiling and prediction tools for use within migration management processes, including for forced deportation. These use cases may infringe on data protection rights, the right to privacy, the right to non-discrimination, and several principles of international migration law, including the right to seek asylum. Given those concerns and the significant power imbalance that such deployments exacerbate and exploit, **there should be a ban or moratorium on the use of automated technologies in border and migration control until they are independently assessed to determine compliance with international human rights standards.**

Predictive policing:

Uses of predictive modelling to forecast where, and by whom, certain types of crimes are likely to be committed repeatedly score poor, working class, racialised and migrant communities with a higher likelihood of presumed future criminality. As highlighted by the European Parliament,[48] deployment of such predictive policing can result in "grave misuse". The use of apparently "neutral" factors, such as postal code, in practice serve as a proxy for race and other protected characteristics, reflecting histories of overpolicing of certain communities, exacerbating racial biases and affording false objectivity to patterns of racial profiling.[49] A number of predictive policing systems have been demonstrated to disproportionately include racialised people[50], in complete

---

45 CNN, *Passengers to face AI lie detector tests at EU airports*, updated 2 November 2018, available at: https://edition.cnn.com/travel/article/ai-lie-detector-eu-airports-scli-intl/index.html

46 Independent, *Government 'deported 7,000 foreign students after falsely accusing them of cheating in English language tests'*, 14 June 2019, available at: https://www.independent.co.uk/news/uk/politics/home-office-mistakenly-deported-thousands-foreign-students-cheating-language-tests-theresa-may-windrush-a8331906.html

47 European Commission, *New Pact on Migration and Asylum – a fresh start on migration in Europe*, available at: https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/new-pact-migration-and-asylum_en

48 European Parliament, Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)), 8 October 2020, available at: https://www.europarl.europa.eu/doceo/document/A-9-2020-0186_EN.html [original footnote]

49 Amnesty International, Netherlands: We sense trouble: Automated discrimination and mass surveillance in predictive policing in the Netherlands (AI Index Nr. EUR 35/2971/2020), 29 September 2020, available at: https://www.amnesty.org/en/documents/eur35/2971/2020/en/ [original footnote]

50 European Network Against Racism (ENAR), Data-Driven Policing: the hardwiring of discriminatory policing practices across Europe (authors: Patrick Williams And Eric Kind), November 2019, available at: https://www.enar-eu.org/IMG/pdf/data-driven-profiling-web-final.pdf [original footnote]
See also the recent report by Fair Trials, Automating Injustice: the use of artificial intelligence & automated decision-making systems in criminal justice in Europe, 2021, available at:

> disaccord with actual crime rates. Predictive policing systems undermine the presumption of innocence and other due process rights by treating people as individually suspicious based on inferences about a wider group. **The European Commission must legally prohibit deployments of predictive policing systems in order to protect fundamental rights.**

Finally, in this sub-section, I should note the criticism of the role of Europol in these developments. As EDRi put it:

> Given the impacts of these assistive technologies on the lives and rights of persons and communities subject to them, … such [a] role [a bigger role in developing and shaping future policing technologies] should not be given to an opaque and unaccountable agency. Instead, we believe the involvement of democratically elected bodies and of representatives of affected groups – mainly marginalised communities - should be actively sought and guaranteed when making decisions over the future of policing tools, practices and strategies.

Here, I merely want to stress that the processing of PNR data under the PNR Directive must be seen in the above wider contexts: the clear and strengthening trend towards more "proactive", "preventive" policing by means of analyses and algorithm/AI-based data mining of (especially) large private-sector data sets and databases; the increasingly central role played by Europol in this (and the proposal to expand that role yet further); the focusing on persons against whom there is (as yet) insufficient evidence for action under the criminal law; and the still increasing intertwining of law enforcement and national security "intelligence" operations in those regards. Moreover, civil society concerns must be taken into account.

- o – O – o –

https://www.fairtrials.org/sites/default/files/publication_pdf/Automating_Injustice.pdf
I will return to these reports in section 4, sub-section 4..9(f), below.

3. Legal standards

There are three different levels of legal standards that are most relevant to the present opinion:

- **general fundamental rights standards**, as laid down in the EU Charter of Fundamental Rights (CFR) and the European Convention on Human Rights (ECHR) in particular;
- **general data protection standards**, as laid down in the EU General Data Protection Regulation (GDPR)and the EU Law Enforcement Directive (LED) in particular; and
- **specific standards relating to risk analyses and profiling**, as set out in the data protection instruments, but as also proposed in relation to artificial intelligence (AI) in the recent European Commission proposal for an Artificial Intelligence Act (AIA).

I will briefly summarise the relevant standards in the sub-sections below.

3.1 General fundamental rights standards (synopsis)

EU attempts to create legal frameworks for bulk access to private sector databases and datasets that are subject to EU law were repeatedly successfully contested in the European and Member States' courts under the EU Charter of Fundamental Rights (CFR) and the European Convention on Human Rights (ECHR).[51]

Thus, as already noted in the previous section, in the CJEU's *Digital Rights Ireland* judgment the Data Retention Directive was held to violate the EU Charter of Fundamental Rights, and mandatory retention of communications data was again held to violate the Charter in *Tele2/Watson*, although the Court introduced a narrow exception for instances of fundamental threats to society in *La Quadrature Du Net*.

Elsewhere,[52] I have provided an analytical overview of these and a series of other cases of the CJEU and of the European Court of Human Rights (ECtHR),[53] and of the European Essential

---

[51] On the issue of access to bulk data sets including the PNR databases by Member States' intelligence agencies, whose activities are as such not subject to EU law, see section 4, sub-section 4.10, below.

[52] Douwe Korff and Ian Brown, submission to various European Union bodies on The inadequacy of UK data protection law in general and in view of UK surveillance laws, *Part Two – UK surveillance law*, section 3.1, Issues and applicable standards, pp. 28 – 36, November 2020, available at: https://www.ianbrown.tech/wp-content/uploads/2020/11/Korff-Brown-Submission-to-EU-re-UK-adequacy-Part-Two-DK-IB201130.pdf

[53] For the overview in the submission, and in the present opinion, I drew on the following case-law:

I. Court of Justice of the European Union judgments and opinion:

- CJEU judgment of 8 April 2014 in 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* (***DRI***);
- CJEU judgment of 6 October 2015 in case C-362/14, *Maximillian Schrems v Data Protection Commissioner* (**Schrems I**);
- CJEU judgment of 21 December 2016 in 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* (***Tele2/Watson***);
- CJEU Opinion 1/15 of 26 July 2017 on the EU – Canada Draft PNR Agreement (***EU-CAN PNR Opinion***);
- CJEU judgment of 16 July 2020 in case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (***Schrems II***);

Guarantees for Surveillance (EEGs), issued by the European Data Protection Board (EDPB), that reflect this case-law.[54] Below, I provide a shortened extract from that overview, setting out the main standards relevant to PNR (with minor edits to relate the summary more closely to PNR, but for reasons of space with the detailed case and EEG references largely omitted).[55]

1. Any form of processing of personal data (including basic data) for intelligence purposes constitutes an interference with fundamental rights:

Any processing of any personal data (including metadata) originally collected and used for other purposes such as commerce, medical treatment, travel, or to facilitate communications, for intelligence purposes constitutes an interference with the fundamental rights of the individuals to which the data relate – the data subjects; this includes mandatory retention of data beyond the normal retention period so as to allow them to be accessed by the intelligence agencies, compulsory active transmission or making available of the data to the intelligence agencies, as well as (more or less passively) allowing those agencies to access or extract such data from the relevant systems (such as servers, cables, bearers or routers). In relation to mandatory data retention, the compulsory retention is one interference; subsequent access to the retained data constitutes a "further" or "separate" interference. Moreover, "[T]he operation of having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data" (*Schrems II*, para. 83).

2. There is already an interference with data subject rights if their data are mandatorily retained – or collected – by law enforcement or intelligence agencies; it is not the

---

- CJEU judgment of 6 October 2020 in joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and others* (***LQDN***);
- CJEU judgment of 6 October 2020 in case C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (**PI**).

II. European Court of Human Rights judgments:

- ECtHR judgment of 6 September 1978 *in Klass and others v Germany* (***Klass***);
- ECtHR judgment of 26 April 1985 in *Malone v the United Kingdom* (***Malone***);
- ECtHR admissibility decision of 29 June 2006 on the application of *Gabriele Weber and Cesar Richard Saravia v Germany* (***Weber and Saravia***);
- ECtHR judgment of 1 July 2008 in *Liberty and others v the United Kingdom* (***Liberty***);
- ECtHR judgment of 18 May 2010 in *Kennedy v the United Kingdom* (***Kennedy***);
- ECtHR judgment of 4 December 2015 in *Roman Zakharov v Russia* (***Zakharov***);
- ECtHR GC judgment of 25 May 2021 in *Big Brother Watch* (***BBW***).

[54] EDPB, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf
The recommendation builds on an earlier WP29 working document, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) (WP237), adopted by the WP on 13 April 2016 in response to the *Schrems I* judgment, but takes into account the important subsequent case-law of both the Luxembourg and Strasbourg Courts, in particular *Schrems II*.

[55] Because of the shortening, the numbers for the various issues listed do not correspond to those in the submission, but the paragraphs and the detailed case- and EEG references are still easy to cross-reference.

case that there is only such an interference if a human agent accesses the retained – or collected and stored – data; that is a "further interference".

This is explicitly stated in *DRI*, paras. 34 – 35 with regard to compulsorily retained data, but the principle clearly also applies to data that are actually collected by law enforcement or intelligence agencies and subjected to automated analysis.

3. All such interferences must be based on "law", be limited to what is strictly "necessary" and "proportionate" to the intelligence purpose in question – which must be a "legitimate" purpose.

(Articles 8 – 11 ECHR; Article 52 CFR)

More specifically:

3.1 ***Re* "law" (1):** The rules under which the interference is authorised must be accessible (i.e., published), legally binding, clear and precise (i.e., "foreseeable" in its application in the sense that "*[t]he domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures*").

References: These are standard requirements under the ECHR and the CFR, reiterated in the EEGs paras. 27 – 31, with reference to CJEU cases Schrems II, paras. 175, 180 and 181, EU-CAN PNR, para. 139 (and further case-law cited there) and PI, paras. 65 and 68; and ECtHR cases Liberty, para. 63, Weber and Saravia, para. 95 and Malone, paras 65 – 66. The quote is from ECtHR judgment in Zakharov, para. 229.[56]

3.2 ***Re* "law" (2):** The law "must itself define" the scope and application of the measure in question.

References: EEGs, para. 29, with reference to the CJEU *Schrems II* judgment, para. 175, repeated *verbatim* with a cross-reference in its *PI* judgment, para. 65, and in its *LQDN* judgment, para. 175. Cf. also its *DRI* judgment, para. 68 (*re* EU law). Repeated in EEGs, para. 36.

Note: In its *BBW* judgment, the ECtHR has outlined "six minimum requirements" that surveillance laws must meet in order to ensure that they are "sufficiently foreseeable to minimise the risk of abuses of power" and which can be said to also indicate the "defining" that the CJEU says should be enshrined in the law itself. These are (in summary):

- [the need for a specification of] the nature of offences which may give rise to an interception order;

[56] The requirements of clarity and foreseeability of legal rules (for which the EDPS in his First Opinion on the proposal for the PNR Directive uses the term "predictability") is a fundamental requirement of the concept of "law" in the European Convention on Human Rights, also adopted by the CJEU. As the ECtHR put it in the seminal judgment on this issue, *Sunday Times v. the UK*, 26 April 1979, at para. 49:
"*Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct.*"

- [the need for] a definition of the categories of people liable to have their communications intercepted;
- [the need for] a [stipulated] limit on the duration of interception;
- [the need for an appropriate] procedure to be followed for examining, using and storing the data obtained;
- [the need for appropriate] precautions to be taken when communicating the data to other parties; and
- [the need for limitations on] the circumstances in which intercepted data may or must be erased or destroyed

(*BBW* judgment, para. 423, summarising the more detailed overview of the six requirements in para. 307, with indents and words in square brackets added. See also the EEGs, para. 30).

The first two of these correspond to the CJEU requirement that there must be some reasonable link between the individuals whose data are collected and the offences or threats to national security in relation to which their data are collected. In other words: **the law itself should expressly preclude the collection of personal data (including basic data) on individuals who have no personal link, or some link in time or place, to the offences or threats in question. General, indiscriminate, "dragnet", bulk collection of personal data (including basic data) – collecting of the "hay" from a "haystack" in order to find a "needle" buried in it – is fundamentally incompatible with EU fundamental rights law; and the laws covering surveillance should themselves, explicitly make clear that such bulk collection is not permitted. This cannot be left to vague language such as instructing a government minister authorising surveillance, or a Member State, to do so only in a "proportionate" manner.**

3.3 ***Re* necessity and proportionality and respect for the essence of rights:** Rules that permit general and indiscriminate transmission of communications data, including basic data to – or access to such data by – law enforcement or national intelligence agencies, are inherently disproportionate and unnecessary, and incompatible with the EU Charter of Fundamental Rights. Rather, there must be some link, "even an indirect and remote one", between the individuals whose data are collected, or the time or place in relation to which the data are collected, and the serious crimes or threats to national security for which the data are collected.

Note: The CJEU judgments on which I drew above focus on the need of there being some personal link between the individuals whose data are collected and the threat in question. In *LQDN*, the CJEU also mentioned exceptional circumstances in which there is **a "serious", "genuine and present or foreseeable" threat to "the essential functions of the State and the fundamental interests of society"** such as "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" (see paras. 135 – 137).

In such extreme situations – comparable to those in which there is a "public emergency threatening the life of the nation" envisaged in Article 15 ECHR, in which many normal human rights guarantees including the right to privacy can be derogated from – the Charter "*does not, in principle, preclude a legislative measure which permits the competent authorities to order providers of electronic communications services to retain traffic and location data of all users of electronic communications systems for a limited period of time*" (para. 137).

However, there must be "sufficiently solid grounds" for considering that such an extreme threat exists. In my opinion, this part of the judgment is clearly limited to "clear and present dangers" to the fundamental functions of the state and cannot be relied upon in relation to lesser threats including isolated acts of terrorism that, while an outrage to the human conscience and a serious threat to individuals, do not threaten those fundamental values or interests. Specifically, I read this as applying in particular to situations in which the authorities learn about a planned serious attack with some indication of the intended time and place – and in which they may therefore decide to indiscriminately monitor (and retain) all traffic and location data of all users of electronic communications systems in the relevant area (cf. *LQDN*, para. 144), for a limited period of time relating to the expected attack. This exception for extreme threats to the foundations of the state and society cannot be relied upon for more general anti-terrorist surveillance. Otherwise, this exception would become the rule – and the Court stresses both earlier in the judgment and shortly after the above paragraphs that derogations from the rights to confidentiality of communication and privacy should never become the rule (see paras. 111 and 142).

4. **Any interference with the right to privacy and data protection, and therefore also any collection and further processing of personal data by law enforcement or intelligence agencies, should be subject to an effective, independent and impartial oversight system that must be provided for either by a judge or by another independent body.**

5. **Individuals whose data have been collected by the intelligence agencies must be notified of this as soon as the notification no longer jeopardizes the tasks for which those authorities are responsible, and must have access to effective remedies before a judicial or quasi-judicial body if they believe their rights have not been respected.**

   (Article 13 ECHR; Article 47 CFR)

   The body must have access to all relevant information including closed materials, and it must have the power to remedy non-compliance with the law (or the above-mentioned standards), i.e., to order remedial action.

6. **If law enforcement or intelligence agencies of EU Member States share data with sister agencies in third countries, then this amounts to a "transfers" of those data to that third country. If that other third country does not provide adequate/essentially equivalent protection to those data, this data sharing/transfer undermines the protection accorded to the data by EU law.**

7. Laws that allow for the taking of decisions on individuals that produce legal effects concerning those individuals or that otherwise "significantly affect" them, "based solely on automated processing, including profiling", must contain "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests". If special categories of personal data are used in this (i.e., data on or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or sexual orientation, or genetic or biometric data), the laws must contain "suitable and specific measures" to safeguard their fundamental rights and interests.

(Article 22(2)(b) and (4), read with Article 9(2)(g) GDPR)

3.2 General data protection standards (synopsis)

This is not the place to discuss EU and Council of Europe data protection standards in detail. Rather, a brief reminder of the main standards that underpin both the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED), will suffice.[57]

Unsurprisingly – indeed intentionally – the main data protection principles fit in neatly with the main fundamental rights standards set out above, at 3.1, in particular the ones relating to **legality** ("based on law"), **legitimate aim**, **necessity** and **proportionality**. To quote the most relevant articles of the Law Enforcement Directive (which is the instrument most directly relevant to the processing of PNR data discussed in this opinion) relating to those principles, with terms that clearly reflect the general human rights standards highlighted:

Article 4

Principles relating to processing of personal data

1. Member States shall provide for personal data to be:

   (a) processed **lawfully** and fairly;
   (b) collected for specified, explicit and **legitimate purposes** and not processed in a manner that is incompatible with those purposes;
   (c) **adequate, relevant and not excessive** in relation to the purposes for which they are processed;
   (d) **accurate** and, where necessary, **kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
   (e) kept in a form which permits identification of data subjects for **no longer than is necessary** for the purposes for which they are processed;

[57] For an overview of the development of data protection in Europe including of the principles summarised in the text, see Douwe Korff and Marie Georges, The Origins and Meaning of Data Protection, January 2020, available at:
https://ssrn.com/abstract=3518386
For a comprehensive commentary on the GDPR including those principles, see C. Kuner, L. A. Bygrave, C. Docksey and L. Drechsler (eds.), The EU General Data Protection Regulation – A Commentary, Oxford University Press, 2020. There is to the best of my knowledge as yet no comparable detailed commentary on the Law Enforcement Directive, but many of the comments in Kuner et al. are either equally applicable to or at least relevant to provisions in the LED.

(f) processed in a manner that ensures **appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2. Processing by the same or another controller for any of the purposes set out in Article 1(1) [i.e., prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security] other than that for which the personal data are collected shall be permitted in so far as:

   (a) the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State **law**; and
   (b) processing is **necessary** and **proportionate** to that other purpose in accordance with Union or Member State **law**.

3. Processing by the same or another controller may include archiving in the public interest, scientific, statistical or historical use, for the purposes set out in Article 1(1), subject to appropriate safeguards for the rights and freedoms of data subjects.

4. The controller shall be **responsible** for, and be able to demonstrate compliance with, paragraphs 1, 2 and 3.

Article 8

Lawfulness of processing

1. Member States shall provide for processing to be **lawful** only if and to the extent that processing is **necessary** for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and that it is based on Union or Member State **law**.

2. Member State **law** regulating processing within the scope of this Directive shall specify at least **the objectives of processing**, the personal data to be processed and the **purposes** of the processing.

Article 10

Processing of special categories of personal data

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be allowed only where **strictly necessary**, subject to **appropriate safeguards** for the rights and freedoms of the data subject, and only:

(a) where authorised by Union or Member State **law**;

(b) to protect the vital interests of the data subject or of another natural person; or

(c) where such processing relates to data which are manifestly made public by the data subject.

Article 11

Automated individual decision-making

1. Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be **prohibited unless authorised by Union or Member State law** to which the controller is subject and which provides **appropriate safeguards** for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.

2. Decisions referred to in paragraph 1 of this Article shall not be based on special categories of personal data referred to in Article 10, unless **suitable measures to safeguard the data subject's rights and freedoms and legitimate interests** are in place.

3. Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited, in accordance with Union law.

Between them, the highlighted terms make clear that any processing of personal data (which *ipso facto* constitutes an interference with the rights to private life and to protection of personal data) by law enforcement authorities (or indeed anyone) must be based on a "**law**" that meets the "quality of law" requirements adduced by the European courts (***accessible***, ***clear***, ***specific*** and ***foreseeable***); that that interference must serve a "**legitimate purpose** in a democratic society"; and that the interference must be limited to what is clearly "**necessary**" and "**proportionate**" to the legitimate purpose in question.

The LED (and the GDPR) build on this by stipulating that personal data must be "**adequate**", "**relevant**" and "**not excessive**" (the GDPR says "**necessary**") in relation to the legitimate purpose in question; that the data must be sufficiently "**accurate**" for that purpose and **kept up to date** if the purpose requires this, and **not retained for longer** (certainly not in identifiable form) **than necessary** for the relevant legitimate purpose; and **protected against data breaches**. Moreover, the LED (and the GDPR) emphasises that "the controller [of the processing] shall be responsible for, and be able to demonstrate compliance with [those standards); this is referred to in the GDPR as the principle of "**accountability**".

The LED (and the GDPR) place even stricter limits on the processing of so-called "**sensitive data**", i.e., of:

> personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, … genetic data, biometric data [if used] for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation …
>
> (Article 10 LED; 9(1) GDPR)

Under the GDPR, the processing of such data is in principle **prohibited**, subject to a series of exceptions that are more tightly drawn than the general principles. For instance, in relation to processing of sensitive data for reasons of public interest, the GDPR stipulates the following:

> [The in-principle prohibition on the processing of sensitive personal data shall not apply when:]
>
> [the] processing is necessary for reasons of **substantial public interest**, on the basis of Union or Member State **law** which shall be **proportionate to the aim pursued**, **respect the essence of the right to data protection** and provide for **suitable and specific measures to safeguard the fundamental rights and the interests of the data subject**
>
> (Article 9(2)(g), emphases added)

The Law Enforcement Directive does not contain an in-principle prohibition on the processing of sensitive data, but is still similarly strict: the **processing of sensitive data** "*shall be allowed only where **strictly necessary***" for any of the purposes set out in Article 1(1) LED, i.e., prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; unless the data were strictly necessary to protect the "vital interests" of the data subject or someone else or the data subject has "manifestly" made the sensitive data public, the processing must be "***authorised by Union or Member State law***" (which of course again must meet the "quality of law" requirements); and even then it must be "***subject to appropriate safeguards for the rights and freedoms of the data subject***".

Note again the strong emphasis on "law", "legitimate purpose" (as specified in Article 1(1)) and "*strict* necessity" (which in this context includes "proportionality"), to which are added a further requirement of "*suitable and specific safeguards*" to protect "*the fundamental rights and the interests of the data subject[s]*".

Under the GDPR, special, especially strict conditions also apply to the processing of **personal data on criminal convictions and offences** (Article 10). Although this is not as clearly stated in the body of the LED, Recital 51 still makes clear that such data must be treated with special caution, also by law enforcement agencies:

> **[Risks] to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead to physical, material or non-material damage, in particular**: … where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs or trade union membership; where genetic data or biometric data are processed in order to uniquely identify a person or **where data concerning** health or data concerning sex life and sexual orientation or **criminal convictions and offences or related security measures are processed** …
>
> (Emphasis added. I have replaced the words "The risk" at the beginning of the recital with the word "Risks" because that is clearly what is intended: cf. the French version that refers to "*Des risques pour les droits et libertés des personnes physiques*". The recital also lists other risks including risks resulting from risk analyses and profiling. I note those separately, below, at 3.3.)

It is strongly arguable that the phrase "criminal offences" includes data suggesting that someone "*may be*" involved in criminal activity: it would make no sense to impose strict conditions on processing of information that says a person is formally suspected of being involved in crime (as typically spelled out in a judicial or prosecutorial order), or indeed

charged with, indicted for or indeed convicted of a crime, but to not impose the same conditions on information in police "**watch lists**" such as lists of "**persons of interest**" that are typically contained in police criminal intelligence files and that say that a person is "suspicious" (as discussed in more detail in section 4, sub-section 4.7, below). There is support for this interpretation in the LED and in the case-law of the European Court of Human Rights. Thus, Recital 13 to the LED expressly stipulates that:

> [The concept of a] criminal offence within the meaning of this Directive should be an autonomous concept of Union law as interpreted by the Court of Justice of the European Union (the 'Court of Justice').

Moreover, in the case of *Khelili v. Switzerland*,[58] the European Court of Human Rights ruled in favour of the applicant who had complained that she was labelled a "prostitute" in police files, even though she had not ever been convicted of that offence. The Court held:

> The Court does not underestimate the importance of effective prevention of crime. Nevertheless, taking into account [the above-mentioned facts] and especially taking into account the fundamental presumption of innocence in a democratic society (…), it cannot accept that the retention of the file entry "prostitute" as the profession of the applicant, who has never been convicted of the illegal exercise of prostitution within the meaning of Article 199 of the Criminal Code (…) can relate to a "pressing social need" within the meaning of Article 8 of the Convention [that protects private and family life].
>
> (para. 68)

The Strasbourg Court similarly held, in *Brunet v. France*,[59] that there had been a violation of Article 8 of the Convention when the applicant's data were retained in a criminal database (the recorded crimes database, "STIC") although the criminal proceedings against him were discontinued.

In other words, processing of information on a person suggesting that that person "*may be*" or "*may have been*" involved in criminal activities is subject to especially strict tests of legitimacy, necessity and proportionality.

3.3 Specific standards relating to risk analyses and profiling

In addition to the above general data protection standards, there are special rules in the data protection instruments on **certain forms of processing that are regarded as posing a "high risk" to the fundamental rights and interests of the data subjects**. Under both the GDPR and the LED, controllers who want to use:

---

[58] ECtHR, 2nd chamber judgment of 18 October 2011 in *Khelili v. Switzerland* (in force from 8 March 2012), available at:
https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-107032%22]}
(My translation as the judgment is only available in French, and in unofficial translations into German, Icelandic and Russian.)

[59] ECtHR, 5th chamber judgment of 18 September 2014 in *Brunet v. France* (in force from 18 December 2014), available at:
https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-146389%22]}
(Only available version is again French.)

> **a type of processing**, in particular, using new technologies, [**that**], taking into account the nature, scope, context and purposes of the processing, **is likely to result in a high risk to the rights and freedoms of natural persons** –

must carry out a **Data Protection Impact Assessment (DPIA)** before commencing the processing (GDPR, Art. 35; LED, Art. 27). If the results of a DPIA "*indicate[ ] that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk*", the controller must consult the relevant supervisory authority (GDPR, Art. 36; LED, Art. 28(1)(a)). Under the LED, the supervisory authority must also be consulted if:

> the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects.
>
> (Article 28(1)(b))

I assume the latter refers to types of processing that *inherently* involve such a "high risk".

The supervisory authority must also be consulted:

> during the preparation of a proposal for a legislative measure to be adopted by a national parliament or of a regulatory measure based on such a legislative measure, which relates to [high risk] processing
>
> (GDPR, Art. 36(4); LED, Art. 28(2))

In 2017, the Article 29 Working Party (WP29), established under the 1995 Data Protection Directive, issued guidelines on DPIAs, that were endorsed by the European Data Protection Board under the GDPR.[60] Under the guidelines, a processing operation is to be regarded as "high risk" if it meets at least two of a series of nine criteria. Briefly, these nine criteria are:[61]

1. **Evaluation or scoring**, including profiling and predicting, especially from "*aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or **behaviour, location or movements***" (recitals 71 and 91) …
2. **Automated decision-making with legal or similar significant effect**: processing that aims at taking decisions on data subjects producing "*legal effects concerning the natural person*" or which "*similarly **significantly affects** the natural person*" (Article 35(3)(a)). …
3. **Systematic monitoring**: processing used to observe, monitor or control data subjects, including data collected through networks or "*a systematic monitoring of a publicly accessible area*" (Article 35(3)(c))15. …
4. **Sensitive data or data of a highly personal nature**: this includes special categories of personal data as defined in Article 9 (for example information about

[60] WP29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP248 rev 1), available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
Endorsed by the EDPB at its first meeting after the coming into effect of the GDPR, on 25 May 2018, Endorsement 1/2018, available at:
https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents_en_0.pdf

[61] For further detail and examples, see the guidelines. For a full discussion, see Douwe Korff, GDPR Requirements on Data Protection Impact Assessments & Methodologies for DPIAs, August 2020, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3656234

individuals' political opinions), as well as **personal data relating to criminal convictions or offences as defined in Article 10**. …

5. **Data processed on a large scale**: the GDPR does not define what constitutes large-scale, though recital 91 provides some guidance. In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:
   a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
   b. the volume of data and/or the range of different data items being processed;
   c. the duration, or permanence, of the data processing activity;
   d. the geographical extent of the processing activity.
6. **Matching or combining datasets**, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject17.
7. **Data concerning vulnerable data subjects** (recital 75): the processing of this type of data is a criterion because of the increased power imbalance between the data subjects and the data controller, meaning the individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable data subjects may include children [and] asylum seekers … , and in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.
8. **Innovative use or applying new technological or organisational solutions** ... The GDPR makes it clear (Article 35(1) and recitals 89 and 91) that the use of a new technology, defined in "accordance with the achieved state of technological knowledge" (recital 91), can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks. …
9. When the processing in itself "***prevents data subjects from exercising a right or using a service or a contract***" (Article 22 and recital 91). This includes processing operations that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract. …

In section 4, sub-section 4.9, below, I will describe in some detail the processing of personal data that is envisaged (or allowed) under the PNR Directive. Here, I may already note that it meets, not just two but effectively (almost) all of the above criteria; it involves:

- evaluating whether a person "may be" involved in terrorism or serious crime, *inter alia* by reference to their behaviour, location and movements;
- the generation of initial "hits" by fully automated data matching;
- the unavoidable systematic monitoring of hundreds of millions (!) of air passengers;

- processing of sensitive data or data of a highly personal nature (if a marking of a person as someone who "may be" involved in terrorism or serious crime constitutes such data, as I argue it does: see above, at 3.2);
- processing of personal data on an enormous scale (see the third indent, above);
- matching of combining of PNR data against (ill-defined) other police and intelligence databases and lists (including SIS);
- processing of large amounts of personal data on vulnerable people such as children;
- innovative uses of new technologies such as algorithm/AI-based profiling; and
- possible prevention of the exercise of individuals' rights, in particular the exercise of the right to freedom of movement.

This means that, contrary to assertions by the European Commission and representatives of EU Member States (*inter alia*, at the hearing in the PNR case in July 2021) that the processing under the PNR Directive has little or no effect on the rights and interests of the data subjects, the processing under the directive in fact undoubtedly poses "high risks" to the fundamental rights and interests of hundreds of millions of airline passengers.

Under the LED (as under the GDPR), this means that the processing should be subject to careful evaluation of the risks and the taking of remedial action to prevent, as far as possible, any negative consequences of the processing – such as the creation of "false positives" (cases in which a person is wrongly labelled to be a person who "may be" involved in terrorism or serious crime). It also means that if it is not possible to avoid excessive negative consequences, the processing is "not fit for purpose" and should not be used.

Under the proposed Artificial Intelligence Act that is currently under consideration, similar duties of assessment and remedial action – or abandoning of systems – are to apply to AI-based processes.[62]

I will return to this in section 4, sub-section 4.12, below, where I will discuss the consequences of a "match" under the PNR Directive, and in my final assessments in section 5.

In this opinion, I will not attempt to assess the PNR Directive, or the laws and practices of the EU Member States under this directive, with reference to each of the above standards. Rather, I will try to assess whether the processing that the PNR Directive requires or allows is suitable, effective and proportionate to the aims of the directive. However, in doing so, in making those assessments, I will of course base myself on the above standards.

- o – O – o -

[62] See: Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021) 206 final), 21 April 2021, available at: https://op.europa.eu/en/publication-detail/-/publication/e0649735-a372-11eb-9585-01aa75ed71a1/language-en/format-PDF/source-205836026

4. The PNR Directive

4.1 Introduction

This section provides an analysis of the PNR Directive ("the directive"),[63] with reference to the European Commission's review report on the implementation of the directive and the staff working document that accompanied that review report.[64] It seeks to note in particular a number of elements or aspects of the directive and the system it establishes that are problematic, either conceptually or in the way they are supposed to operate or to be evaluated, to which I return in section 5.

NB: This opinion focusses on the system as it is designed and intended to operate, and on what it allows (even if not everything that may be allowed is [yet] implemented in all Member States), and less on the somewhat slow implementation of the directive in the Member States and on the technical aspects that the Commission report and the staff working document often focussed on. It notes in particular a number of elements or aspects of the directive and the system it establishes that are problematic, either conceptually or in the way they are supposed to operate or to be evaluated.

4.2 The system

The PNR Directive creates an infrastructure for:

(a) the **collection** of data contained in so-called (airline) passenger name records ("PNR data") by airlines and the **passing on** of those data (by "***push***" method) to special **Passenger Information Units (PIUs)** that the PNR Directive requires each EU Member State to establish (Art. 4);

(b) the (mostly) **fully automated matching** of the PNR data by the PIUs against various *lists* in order to identify individuals already "*known*" to be involved in terrorism or other serious crime, and against so-called "*pre-determined criteria*" to "identify" *previously unknown* individuals who "may be" involved in terrorism or certain other forms of serious transnational crime;[65] if there is a match this produces what I will call an "**initial hit**";[66]

(c) a **manual check** of the initial "hits" by the PIUs; if the PIU staff is satisfied that the initial "hit" is correct, this leads to a **confirmed "hit"**; *

* I discuss the criteria for judging whether an initial "hit" should be considered a confirmed "hit"/positive result in sub-section 4.9, below: this differs according to the different kinds of matches.

---

63 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4 May 2016, pp. 132 – 149, available at: https://eur-lex.europa.eu/eli/dir/2016/681/oj

64 See footnote 5, above.

65 I discuss the different meanings of the word "identify" in sub- section 4.9, below.

66 I discuss the distinction between **initial "hits"** generated by the initial (mostly automated) matching and **confirmed "hits"** in sub-section 4.9, below; see in particular the discussion in sub-section 4.9(a). In the evaluation of the operation of the Dutch PNR law (footnote 6, above), the initial "hits" are called "matches" and the confirmed "hits", "hits"; and a further distinction is made with "alerts", i.e., the passing on of the confirmed "hits" to the competent authority by an in-between body created there, the *Frontoffice* that further checks and "enriches" the "hits" confirmed by the Dutch PIU staff. Because the latter is a particularity of the Dutch system, and because the use of the term "alert" can cause confusion in relation to matches against SIS alerts (which are fundamentally different), I am not following that terminology.

(d) **analysis** of the data by the PIU staff (and others)[67] ***to refine the "pre-determined criteria" and develop new criteria***;

(e) the **passing on** of PNR data and of the results of the analyses, by the PIUs acting on their own initiative, to "competent authorities" in the PIU's own country for "further examination" when the matching process within the PIU produces a confirmed "hit";

(f) the **sharing** of PNR data and of the results of the analyses between the PIUs of the EU Member States;

(g) the **provision** of PNR data to competent authorities or Europol **on request**; and

(h) the **transfer** of PNR data to third countries **on a case-by-case basis**.

The PIUs are central to the system:[68]

> The Passenger Information Unit is the core of the PNR mechanism. The Passenger Information Unit is a dedicated unit set up to receive PNR data from the air carriers. Each Member State must establish a Passenger Information Unit (Article 4.1). The Passenger Information Unit is the 'guardian' of the PNR database, in the sense that only its staff should have access to all the PNR data collected. The Passenger Information Unit is responsible for conducting the initial assessment of PNR data and sending the results of their processing to law enforcement authorities at the national level (the 'competent authorities', in the Directive's terminology) as well as for exchanging PNR with the Passenger Information Units of other Member States and with Europol (Article 4.2). Member States are also required to adopt a list of competent authorities entitled to request or receive PNR data and the results of processing such data from the Passenger Information Unit.

I discuss the dissemination of the data in sub-section 4.10, below. Here, I should note in relation to the above brief section from the Commission staff working document: (i) that the "competent authorities" to which data may be send include **not only law enforcement agencies *stricto senso*, but also, in many Member States, the states' intelligence agencies** (see sub-section 4.5, below); and (ii) that **in some Member States the PIUs are actually "embedded in … [the] state security agenc[ies]"**[69] – something rather omitted from the above section in the working paper.

The above provisions and exchanges of data are undoubtedly important to identify "known" persons listed in various databases and lists, by matching the data in those with PNR data.

However, these kinds of matches are rather peripheral to the other main aim of the system, which **is to facilitate data analysis to detect "suspicious" patterns and "unknown" persons and connections, for "criminal intelligence" purposes**:[70]

> The analysis of [PNR] information can provide the authorities with important elements from a criminal intelligence point of view, allowing them to detect suspicious travel

---

67 See sub-section 4.9(fc), below.

68 Staff working document (footnote 5, above), section 3.3, on p. 6.

69 *Idem*, section 5.3, on p. 23.

70 *Idem*, Introduction, p. 2.

> patterns and identify associates of criminals and terrorists, in particular those previously unknown to law enforcement authorities.

I will discuss the different aims of the PNR system in more detail below, at 4.3, and the different matches at 4.9. Here, it will suffice to note that:

It is clear from the staff working document that the "spontaneous" and "on request" transfers of personal data relate mainly to specific checks on, or specific searches for, "known" individuals (or goods).

However, the at least as important – and much more controversial – other aim of the directive is the "pro-active" and "preventative" discerning of patterns, in particular travel patterns, to create "pre-determined criteria" (i.e., profiles)[71] that can be used to "identify"[72] previously "unknown" "persons of interest".[73]

In this paper, I will try to assess whether the PNR Directive is suitable, effective and proportionate in relation to the aims it seeks to achieve.

Those aims are therefore the first issue to be discussed. After that, I will look at the legal bases for the directive (which depend on those aims); the main recipients of the data (the "competent authorities" in the Member States); the crimes in relation to which the system is used; the categories of data subjects and of personal data covered; the kinds of checks and analyses that are performed; the different transfers of the data; and the consequences of the checks. In section 5, I will base my assessments of the suitability, effectiveness and proportionality of these elements, and of the system overall, on the analyses in this section, in the light also of crucial statistical matters noted in sub-section 4.9(f).

4.3 The aims of the PNR Directive

The directive and the Commission report and staff working document are oddly somewhat ambiguous about the aims and purposes of the PNR Directive and the system it establishes.

The **overall aim** of the directive is made clear in its very title; it seeks to enable:

> the use of passenger name record (PNR) data for **the prevention, detection, investigation and prosecution of terrorist offences and serious crime**.[74]
>
> (emphasis added)

Or as set out in some more detail in recital (5):

> The objectives of this Directive are, *inter alia*, **to ensure security, to protect the life and safety of persons, and to create a legal framework for the protection of PNR data with regard to their processing by competent authorities**.
>
> (emphasis added)

---

71 On the use of that term, see Box 3 on p. 69, below.

72 On the use of that term, see sub-section 4.9, below.

73 On that category of individuals, see sub-section 4.7, *The categories of data subjects affected*.

74 In section 4.6, below, I will note that the range of "serious crimes" is actually quite wide and ill-defined.

The "inter alia" is somewhat odd but presumably not intended to widen the scope of the directive beyond the matters listed (security, protection of life and safety, and data protection); it presumably refers to ancillary technical matters that are also regulated by the directive. More importantly, although this is not very clearly spelled out in the directive itself, **the main aim of the PNR Directive is to provide intelligence on terrorism and serious crime and to analyse PNR data in order to identify various patterns and to create profiles (referred to as "pre-determined criteria") that can then help to actually fight those evils**:[75]

> The content of PNR data varies depending on the information given by the passenger and may include, for example, dates of travel and travel itinerary, ticket information, contact details like address and phone number, travel agent, payment information, seat number and baggage information. **The analysis of such information can provide the authorities with important elements from a criminal intelligence point of view, allowing them to detect suspicious travel patterns and identify associates of criminals and terrorists, in particular those previously unknown to law enforcement authorities.**

This is in contrast to the Directive 2004/82/EC (the API Directive)[76] that already imposed an obligation on airlines to communicate passenger data to Member States and that:

> aims at **improving border controls and combating illegal immigration** by the transmission of advance passenger data by carriers to the competent national authorities.
>
> (API Directive, Article 1)

As the European Data Protection Supervisor noted in his first opinion on the proposal for the PNR Directive, with reference to the Explanatory Memorandum to the proposal:[77]

> **Identification of purpose**
>
> Contrary to Advanced Passenger Information (API) data that are supposed to help identifying individuals, PNR data mentioned in the proposal would contribute to **carrying out risk assessments of persons, obtaining intelligence and making associations between known and unknown people**. …
>
> The wording of the proposal and its impact assessment indicate that **the objective is not simply to identify known terrorists or known criminals involved in organised crime, by comparing their names with those included in lists managed by law enforcement authorities. The purpose is to gather intelligence with regard to terrorism or organised crime, and more precisely 'to carry out risk assessment of persons, obtain intelligence and make association between known and unknown**

---

75 Staff working document (footnote 5, above), 1. Introduction, p. 2, emphasis added.

76 Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L 261, 6 August2004, p. 24ff, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2004.261.01.0024.01.ENG&toc=OJ%3AL%3A2004%3A261%3ATOC

77 EDPS, (First) Opinion of the European Data Protection Supervisor 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, 25 March 2011, paras. 6 and 13 – 16 (heading "*Identification of purpose*" moved from just above para. 13 to also cover para. 6), emphasis added, available at: https://edps.europa.eu/sites/default/files/publication/11-03-25_pnr_en.pdf

> **people'.[78] The purpose stated in Article 3(5) of the proposal is, in the same line and firstly, 'to identify persons who are or may be involved in a terrorist or organised crime offence, as well as their associates.'**
>
> This is the reason invoked to explain that API data are not sufficient to reach the alleged purpose. Indeed, as already mentioned, while API data are supposed to help identifying individuals, **PNR data do not have an identification purpose, but the details of the PNR would contribute to carrying out risk assessments of the persons, obtaining intelligence and making associations between known and unknown people**.
>
> The purpose of the measures envisaged does not only cover the catching of known persons but also the locating of persons that may fall within the criteria of the proposal.
>
> **In order to identify these persons,[79] risk analysis and identification of patterns are at the core of the project.** Recital 9 of the proposal states explicitly that data must be kept 'for a sufficiently long period as to fulfil the purpose of developing risk indicators and establishing patterns of travel and behaviour'.
>
> The purpose is thus described in two layers: the first layer consists of the global objective to fight against terrorism and organised crime, while the second layer includes the means and measures inherent to the achievement of this objective. While the purpose of fighting terrorism and organised crime appears to be clear enough and legitimate, the means used to reach this purpose leave room for discussion.

I will discuss the differences between PNR data and API data, and the implications for the use and analyses of those data, in sub-sections 4.8 and 4.9, below.

Here, it will suffice to note that, **in simple terms, <u>the overall aim</u> of the PNR Directive is to facilitate the apprehension of terrorists and individuals who are involved in other serious transnational crime, including in particular international drug- and people trafficking and illegal migration, not just by identifying "known" terrorists and serious criminals, but also and in particular by means of "risk analyses" and the identification of "patterns" (and, we may add, the creation of "profiles" based on the identified patterns)[80] to "identify" previously "unknown" (possible or probable) terrorists and other serious criminals.**

However, **<u>the first aim of the checking of the PNR data by the PIUs is more limited than the aims of the directive overall</u>**: this is:[81]

> **<u>to identify persons who require further examination</u>** by the competent authorities referred to in Article 7, and, where relevant, by Europol in accordance with Article 10,

---

78 Explanatory Memorandum of the proposal, Chapter I. [original footnote]

79 I would put the word "identify" in this context in quotation marks. See sub-section 4.7.

80 I will note the question of whether the patterns and criteria used constitute "profiles" in sub-section 4.9(f), below: see <u>Box 2</u> on p. 72. But here, I may already agree with the EDPS when he says that "*Whether or not it is officially recognised that the proposal aims at profiling passengers, the main point at stake is not about definitions. It is about the impact on individuals.*" (First Opinion on the proposal for the PNR Directive, footnote 77, above, para. 21).

81 The other two aims, as also set out in Article 6(1), are: to provide competent authorities and (in certain circumstances) Europol with PNR data and/or the results of data analyses on request, and to carry out analyses of the PNR data in order to update previously used "pre-determined criteria" used in the "identification of persons who require further examination" and to create new criteria. On these, see sub-sections 4.10 and 4.9(fc), below, respectively.

> **in view of the fact [?] that such persons may be involved in a terrorist offence or serious crime**.
>
> (Article 6(1)(a), emphases and question mark in brackets added)

In sub-sections 4.6, 4.7 and 4.9 and section 5, below, I will discuss this rather strange phrase, and in particular the dangerous ambiguity of the terms "*persons who may be involved in a terrorist offence or serious crime*" and "*identify*", in more detail.

Here, I will merely already note that **the suitability, effectiveness and proportionality of the PNR Directive cannot and should not be assessed by reference to the number of initial "hits" noted by the PIUs, compared to the number of cases passed on for "further examination" to the competent authorities, but rather, that the suitability, effectiveness and proportionality of the directive should be assessed with reference to more concrete outcomes** – although it is not easy to choose the most appropriate outcome point of reference for this exercise, as discussed later. In section 4, sub-section 4.9(fe), at (i), I will note that the discussions at the Court hearing in July 2021 wrongly focussed on this erroneous point of reference (the percentage of cases in which there was a "hit" that were passed on for "further examination"). ***That was a fundamental error.***

4.4 The legal bases for the PNR Directive

The PNR Directive makes clear, in its very first introductory sentence, that it is based on Articles 82(1)(d) and 87(2) of the Treaty on the Functioning of the European Union (TFEU). Questions have arisen as to whether these are the appropriate legal basis for that directive. There is no mention of Article 16 TFEU that deals with data protection.

The legal basis of any directive depends on the aims and purposes of the directive in question. In the previous sub-section, I have concluded that the aim of the PNR Directive, as set out in the very title of that directive itself, is to allow and facilitate "*the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*".

In the CJEU's Opinion on the EU-Canada PNR agreement, the Court addressed precisely this issue, as follows:[82]

> **The appropriate legal basis having regard to the FEU Treaty**
>
> Having regard to the foregoing considerations, the decision on the conclusion of the envisaged agreement relates, in the first place, directly to the objective pursued by Article 16(2) TFEU.
>
> That provision constitutes, without prejudice to Article 39 TEU, 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 FEU Treaty relating to judicial cooperation in criminal matters and police cooperation, as is confirmed by Article 6a of

[82] CJEU (Grand Chamber), *Opinion 1/15 of 26 July 2017 on the Draft Agreement between Canada and the European Union on Transfer of Passenger Name Record data from the European Union to Canada*, ECLI:EU:C:2017:592, paras. 95 – 104, emphases added, available at: https://curia.europa.eu/juris/document/document.jsf?docid=193216&doclang=EN

Protocol No 21 and Article 2a of Protocol No 22, and the Declaration referred to in paragraph 32 of this Opinion.

It follows that the Council decision on the conclusion of the envisaged agreement must be based on Article 16 TFEU.

In the second place, that decision must also be based on Article 87(2)(a) TFEU. That provision states that, for the purposes of Article 87(1) TFEU, according to which the Union is to 'establish police cooperation involving all the Member States' competent authorities', the Parliament and the Council may establish measures concerning 'the collection, storage, processing, analysis and exchange of relevant information'.

In this connection, it should be observed, first, that relevant information, within the meaning of Article 87(2)(a) TFEU, in relation to the prevention, detection and investigation of criminal offences, may include personal data and, second, that the 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.

In this instance, the envisaged agreement establishes, inter alia, rules governing both the transfer of PNR data to the Canadian Competent Authority and the use of that data by that authority. That authority is, in accordance with Article 2(d), read in conjunction with Article 3(1) of that agreement, competent to process PNR data for the purpose of preventing, detecting, investigating or prosecuting terrorist offences or serious transnational crime. Furthermore, Article 6 of that agreement provides that Canada is to share, as soon as is practicable, relevant and appropriate analytical information containing PNR data with Europol and Eurojust and the judicial and police authorities of a Member State. Article 6 also provides that, at the request of those agencies and authorities, Canada is to share PNR data or analytical information containing such data, in specific cases, for the purpose of preventing, detecting, investigating or prosecuting within the European Union a terrorist offence or serious transnational crime. As the Advocate General has observed in points 105 and 106 of his Opinion, the agreement therefore concerns the processing and exchange of relevant information within the meaning of Article 87(2)(a) TFEU and also relates, as is clear, inter alia, from paragraph 80 of this Opinion, to the objective set out in Article 87(1) TFEU.

In those circumstances, the fact that PNR data is initially collected by air carriers for commercial purposes and not by a competent authority in relation to the prevention, detection and investigation of criminal offences does not, contrary to what the Parliament claims, preclude Article 87(2)(a) TFEU from also constituting an appropriate legal basis for the Council decision on the conclusion of the envisaged agreement.

By contrast, that decision cannot be based on point (d) of the second subparagraph of Article 82(1) TFEU, which provides for the possibility for the Parliament and the Council to adopt measures to 'facilitate cooperation between judicial or equivalent authorities of the Member States in relation to proceedings in criminal matters and the enforcement of decisions'.

As the Advocate General has observed in point 108 of his Opinion, none of the provisions of the envisaged agreement refer to facilitating such cooperation. As for the

> Canadian Competent Authority, that authority does not constitute a judicial authority, nor does it constitute an equivalent authority.
>
> In those circumstances, having regard to the case-law cited in paragraph 77 of this Opinion, the Council decision on the conclusion of the envisaged agreement should be based on both Article 16(2) and Article 87(2)(a) TFEU, unless such a combination of legal bases is not possible in accordance with the case-law referred to in paragraph 78 of this Opinion.

In my opinion, it appears obvious from the Court opinion on the Draft EU-Canada Agreement that the PNR Directive, too, should have been based on Articles 16 and 87(2)(a) TFEU, and not on Article 82(1) TFEU.

Moreover, as the Court explains with regard to that draft agreement, the erroneous choice of legal basis for that draft agreement meant that the proper legislative procedure was also not followed: see paras. 105 – 118.

It follows that the PNR Directive, too, appears to not have been adopted in accordance with the properly applicable procedure.

That could lead to the directive being declared invalid on that ground alone – but I will leave that aside for now and will still continue with my assessment of the substance of the directive.

4.5 The competent authorities

As explained in the staff working document:[83]

> Article 7 of the PNR Directive requires Member States to 'adopt a list of the competent authorities entitled to request or receive PNR data or the result of processing those data from the Passenger Information Unit'. It also provides that such authorities 'shall be competent for the prevention, detection, investigation or prosecution of terrorist offences or serious crime'. All Member States have already established a list of competent authorities and notified it to the Commission.
>
> Almost all Member States have appointed the police and other relevant authorities for crime prevention and the protection of public order as competent authorities. In addition, **national transposition measures in many Member States designate intelligence services, including military intelligence services, as authorities competent to receive and request PNR data from the Passenger Information Unit.**[84] Less than half include the judicial authorities on their list of competent authorities, mainly the State Prosecutor's Office and, in some cases, the courts. The vast majority of Member States have also designated customs as a competent authority, whereas only a few have done so for the financial authorities (when responsible for investigation of fraud, money laundering or other financial crimes).

In fact, as already noted at 4.2, above, **in some Member States the PIUs are actually "embedded in … [the] state security agenc[ies]"**[85]

---

83 Staff working document (footnote 5, above), section 3.6, p. 8, emphasis added.

84 The text of a footnote here in the staff working document is quoted in the text.

85 See sub-section 4.2 and footnote 69, above.

The phrase "the result of processing [of PNR data]" clearly includes also the outcomes of the analyses of the PNR data (by the PIUs working with others: see sub-section 4.9(fc), below) and the new or improved "pre-determined criteria" and profiles that are generated as a result.

The document adds in a footnote (footnote 39) that the designation of intelligence services as "competent authorities":

> is compatible with the PNR Directive to the extent that these services use PNR data only for the specific purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious crime (Article 7.4), i.e. [provided that they] respect[ ] the purpose limitation of the Directive.

However, there is no information on how respect for this limitation is ensured in practice.[86]

Given the increasingly close cooperation between law enforcement and intelligence agencies (and border agencies), in particular in relation to the mining of large data sets and the development of evermore sophisticated AI-based data mining technologies by the agencies working together (and in future especially also with and through Europol, more especially in the development of these technologies: see section 2, sub-section 2.3, above), this involvement of the intelligence agencies (and in future, Europol) in PNR data mining must be seen as a matter of major concern. I will return to this in sub-section 4.9(f) and section 5, below.

4.6 The crimes covered ("PNR-relevant offences")

I noted in sub-section 4.3, above, that in simple terms the overall aim of the PNR Directive is to facilitate the identification and apprehension of individuals who are involved in terrorism or other serious transnational crime (and to obtain intelligence in relation to such crimes). It is important to be aware of the scope of these offences (also, again, not least in order to be able to assess the suitability, effectiveness, and proportionality – or otherwise – of the use of PNR Data).

At the time of adoption of the PNR Directive, "**terrorist offences**" *stricto senso* and related and ancillary offences ("offences relating to a terrorist group"; "offences linked to terrorist activities"; and "aiding or abetting" those other offences) were defined in Articles 1 – 4 of Council Framework Decision 2002/475/JHA[87], and the directive therefore cross-referred to those articles in that decision in Article 3(8). However, Framework Decision 2002/475/JHA has been replaced by a directive, Directive 2017/541,[88] which in its Articles 3 – 12 significantly extended the list of "terrorist offences" and related and ancillary offences, in particular in

---

[86] In the Netherlands, the intelligence agencies apparently have direct access to the bulk PNR data – which is contrary to the CJEU case-law summarised at 3.2, above, as I will note in sub-section 4.10, below

[87] Council Framework Decision of 13 June 2002 on combating terrorism, OJ L 164, 22 June 2002, p 3ff, available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002F0475

[88] 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 March 2017, pp. 6–21, available at:
https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32017L0541

relation to travelling for the purpose of terrorism. The concept of "terrorist offences" as used in the PNR Directive should now be read as including all the offences in those 10 articles.[89]

The concept of "**serious crime**" is defined in the PNR Directive with reference to an annex (Annex II); the directive applies to the offences listed in that annex, insofar as they are "*punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State.*" (Article 3(9)).

Attachment 1 to this paper lists all the offences mentioned above: those in Article 3 – 12 of Directive 2017/541, and Article 14 in that directive that covers aiding and abetting, inciting and attempting of those offences, and those in Annex II to the PNR Directive. The lists are extensive.

The main offences included in the lists – murder, kidnapping, hijacking of planes, making bombs, rape, trafficking in human beings, arms, stolen cars or drugs, sexual abuse of children and child pornography, etc. – are undoubtedly serious. However, the activities are often so widely described that inevitably relatively minor acts will also be caught – and this is not fully mitigated by the stipulation that these acts must be punishable by at least three years' imprisonment.

For instance, "fraud" (PNR Directive, Annex II, point 7) is a very wide term, and will almost everywhere carry a maximum penalty of more than three years – but includes relatively trivial acts for which any actual penalties imposed would be minor, e.g., if someone tried to enter a concert by knowingly using a fake ticket, or travelled on a train with a ticket on which the date had been altered. The concepts of "computer-related crime" and "cybercrime" (PNR Directive, Annex II, point 9) are undefined but must be assumed to include the offences listed in the Cybercrime Convention (also known as the Budapest Convention), which includes "hacking" ("accessing a computer system without right") and infringement of copyrights and related rights. Recording a film shown on television onto a DVD can constitute "piracy of [a] product[ ]" (PNR Directive, Annex II, point 17) – and if the DVD is sold or even given to someone else, this may well constitute an act that is in principle punishable by more than three years.

It is easy to think of similar examples of minor breaches of rules against imports of endangered plant species, antiques, art, hormonal substances, etc., or against "facilitation of unauthorised residence" (letting out a house or flat to an illegal migrant?). I note in particular that the term "trafficking" is not itself defined – in particular, there is no indication that the

[89] It is of interest to note that Article 3 of Directive 2017/541 effectively contains a definition of "terrorism", i.e., the commission of any of the offences listed in para. (1) of that article, when committed for the purposes listed in para. (2): seriously intimidating a population; unduly compelling a government or an international organisation to perform or abstain from performing any act; or seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation. There is nothing in this to exclude states from the scope of the directive, and from liability for the acts described when committed for those purposes (and it is undeniable that some states engage in such acts, for such purposes). Indeed, the directive expressly stresses that "legal persons" can be liable for terrorist offences. Although the focus in that regard is clearly on entities such as companies (cf. Art. 18), states are undoubtedly also legal entities, under both international law and the laws of all countries. But this will not be further discussed in this paper.

relevant crimes ("trafficking in human beings", "illicit trafficking in narcotic drugs and psychotropic substances", "illicit trafficking in weapons, munitions and explosives", etc.) are limited by the use of this term to major, organised activities, to the exclusion of minor acts by individuals acting alone (e.g., a tourist bringing home an antique carpet).[90]

Anti-terrorist legislation, and in particular offences such as "incitement" or "support" for terrorism or organisations declared to be terrorist organisations, have also often been applied excessively.[91]

Two further matters should be noted in this regard. The first is that the lists against which the PNR data can be checked by the PIUs, including in particular SIS alerts including alerts relating to European Arrest Warrants (and "national law enforcement repositories" that contain similar matters), are not limited to the offences in relation to which the PNR data are (only) supposed to be used (referred to in the staff working document as "**PNR-relevant offences**"). Specifically, as noted in section 2, sub-section 2.3, above, SIS alerts and EAWs can relate to offences carrying a maximum sentence of at least 12 months imprisonment, whereas (as noted above) "PNR-relevant offences" are limited to offences carrying a maximum sentence of at least 3 years' imprisonment.

Secondly, if a Member State's competent authorities, in the course of seeking to prevent, detect, investigate or prosecute terrorist offences or serious crime on the basis of PNR data (or of the results of analyses of those data by the PIUs), happen to come across evidence of lesser crimes (crimes not within the – already broad – list in Annex I, or while within the scope of the list, not punishable by more than three years: so-called "**not PNR-relevant offences**"), they can still use the PNR data (or the analysis data) to pursue those lesser crimes (Article 7(5)).

Not only does this create **a loophole in the system** – it also **creates a serious dilemma under the PNR Directive** for states that do not want to, or legally cannot, use this loophole, as further discussed in sub-section 4.9(a), below.

---

[90] Some of the crimes are limited in other ways than through the term "trafficking". For instance, EU Directive 2011/36/EU defines human trafficking as "The recruitment, transportation, transfer, harbouring or receipt of persons, including exchange or transfer of control over that person, *by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation*." However, there do not appear to be any such restrictions on the concepts of "trafficking in cultural goods", defined simply as "the illicit import, export and transfer of ownership of cultural property (items of importance for archaeology, prehistory, history, literature, art or science)." See:
https://ec.europa.eu/culture/cultural-heritage/cultural-heritage-eu-policies/protection-against-illicit-trafficking
"Trafficking in stolen vehicles" appears to also not be restricted to organised thefts and illegal exports of cars.

[91] See the Joint Declaration on Defamation of Religions, and Anti-Terrorism and Anti-Extremism Legislation by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression and the ACHPR (African Commission on Human and Peoples' Rights) Special Rapporteur on Freedom of Expression and Access to Information, Athens, 9 December 2008, available at:
http://www.oas.org/en/iachr/expression/showarticle.asp?artID=735&lID=1
https://www.osce.org/files/f/documents/4/b/35639.pdf

Here, it will suffice to note that **the vagueness and relative open-endedness of the lists of offences in relation to which PNR can be used mean that the application of the directive in practice is not foreseeable – which raises serious doubts as to whether it constitutes "law" in the European sense.**[92] **That vagueness also makes it difficult to assess the suitability, effectiveness or proportionality of the directive.** I will return to this latter complication in section 5, below.

4.7 The categories of data subjects targeted and the meaning of (confirmed) "hits"

The PNR Directive covers all the **approximately one billion (!) PNRs** on all passengers on all extra-EU flights and almost all passengers on intra-EU flights.[93] In sub-section 4.9(f), I conclude that this roughly (conservatively) covers **some 500 million individuals** (there taken as the "base rate" for statistical analysis). Within this extremely wide category, there are smaller categories of groups relevant to the processing of PNR data that can be described, in diminishing order, as:

0. (anyone who "may be" involved in terrorism or other serious crime ["PNR-relevant crime"]);*

   * As discussed below, this is not really a sub-category of all air passengers, hence the brackets and the number "0")

1. all persons who are listed by law enforcement or intelligence services as a "person of interest", and within that category, all persons who are so labelled in relation to terrorist or other serious crimes ("PNR-relevant crimes");

2. all persons who are pro-actively "identified" (read: labelled) by the PIUs as a person who "may be involved in terrorism or other serious crime" because their data matches certain "pre-determined criteria" – but who are not (yet) under formal criminal investigation or sanction;

3. all persons who are under formal criminal investigation or sanction under criminal- or criminal procedure law in relation to PNR-relevant crimes (i.e., all persons formally declared to be *suspected* of involvement in such crimes; all persons formally *wanted* for such offences; all persons formally *charged* with such offences; all persons actually *prosecuted* for such offences; and all persons actually *convicted* of such offences – to which I will refer collectively as "**formally wanted persons**"); and

4. any actual terrorists or other serious criminals that for some reason are not included in any of the previous categories.

These categories deserve some clarification. The first (non)category (numbered "0") – "*anyone who 'may be' involved in terrorism or serious crime*" – is not really a sub-category of the overall group of all air passengers: in principle, any air passenger (indeed anyone) "*may*

92 See section 2, sub-section 2.5 and footnote 56, above.

93 According to Eurostat, in 2019, 1,034 million people in the EU travelled by air; in 2018 the number was just under 1,000 million. See:
https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Air_transport_statistics
The figures for 2020 are not in the normal range because of the Covid-19 pandemic.

be" a terrorist or serious criminal. It must be distinguished from the second proper sub-category: persons who are "identified" by the PIUs as persons who "may be" involved in terrorism or serious crime. Before discussing that category, I should note however an even broader one, that of persons who are listed by law enforcement or intelligence agencies as "*persons of interest*" – or "*subjects of interest*" as they are known in the UK.

In its evidence to a UK House of Commons select committee, the UK foreign intelligence service, SIS (more commonly known as MI6), explained that this category simply covered all "*people that we believe that we have an interest in*".[94] The category is rather coyly only mentioned in this sense once in the staff working document:[95]

> [L]aw enforcement authorities from across Member States have indicated that PNR data has been successfully used to … obtain full details of **persons of interest** [and to] identify **previously unknown suspects** …

In this context, it is useful to recall that the Member States' intelligence agencies can (through other agencies) issue a **"discreet check" alert** on the SIS database when they believe they have some "concrete indication" that a person poses a serious threat – but where there is (as yet) not enough information to designate that person formally under criminal (procedure) law as a suspect of a (serious) crime (let alone to arrest, charge or convict him or her), and that law enforcement agencies in practice issue similar "Article 36" alerts against such still-presumed-to-be-innocent people. As noted in section 2.3, above, **in the Netherlands 82.4% of all confirmed "hits" were "hits" against this category of "persons of interest".**

The problem with this category – (however it is named: "*persons of interest*", "*subjects of interest*", "*persons in relation to whom there are 'concrete' [but not really very substantial] indications that they pose a threat*", or in relation to SIS, "*persons subject to an Article 36 alerts*") – is that it is ill- (in fact, not really) defined and essentially self-referential: a person is "identified" as a "person of interest" because the authorities believe that the person is of interest.

The same applies to a considerable extent to the category of persons who are "identified" as "*a person who may be involved in terrorism or other serious crime*". Essentially, this is a label that is attached to the person because a PIU feels that attaching the label is justified. It would appear that the basis for such a decision – for the attaching of the label – is that there was a "hit" of the data in the PNR database against the data sets, lists and criteria that the PNR data are matched against, provided that (in particular if the initial "hit" resulted from automated processing) the initial "hit" was confirmed after a manual check.

In fact, there are fundamental distinctions between different kinds of "hit": if a person is identified through the matching of "hard" identity data (full name, date of birth,

---

[94] See UK House of Commons' Intelligence and Security Committee, Privacy and Security: A modern and transparent legal framework (HC 1075) ("**ISC report**"), 12 March 2015, paras. 20 and 152, available at: http://isc.independent.gov.uk/news-archive/12march2015

[95] Staff working document (footnote 5, above), section 3.6, on p. 9, emphasis added. The document mentions a "*person of interest*" in one other context, in its "*Case studies illustrating the use of PNR data collected on intra-EU flights*", on p. 25, but in that case the person was actually already the subject of a European Arrest Warrant, and therefore falls in category 4, "*persons formally wanted for [relevant] offences*".

nationality/citizenship) as a formally wanted person, or even as a "person of interest" on an intelligence list, that means that the person is (almost certainly) the wanted person or "person of interest". By contrast, "identifying" a person as a "possible terrorist" or "possible serious criminal" on the basis of "pre-determined criteria" or profiles, amounts to no more than the attaching of a probability score to that conclusion (and the score can be quite low, as I will show in sub-section 4.9(f) in particular).

In sub-section 4.9, below, I will therefore argue that while some confirmed "hits" can be regarded as "positive results" of the data matching discussed in that sub-section, others should not. I discuss this further in section 5, sub-section 5.2(ab). Here, it will suffice to note that:

The difference between identifying formally wanted persons by simple data matching (category 3) and "identifying" persons as possibly being terrorist or serious criminals, or even just "of interest", on the basis of vague indications and probability scores (categories 1 and 2) is fundamental – and has fundamental implications in relation to the issue of whether the relevant checks are suitable, effective and proportionate, as further discussed in sub-section 4.9 and in section 5, sub-section 5.2, below.

As also further discussed in sub-section 4.9(f) and in section 5, below, it is difficult to put precise figures on the vague categories 1 and 2 (except that there are certainly less persons in these categories combined than the total numbers of initial and confirmed "hits") – and even data on category 3 are often hard to come by. And no-one really knows the number of people in the 4th category: actual terrorists that for some reason are not included in any of the previous categories, and not flagged up in the PNR checks.

This, yet again, makes it difficult to assess the suitability, effectiveness and proportionality (or otherwise) of the processing under the PNR Directive.

4.8 The categories of personal data processed

(a) PNR data

The PNR Directive provides the following definition of PNR data:

> '**passenger name record**' or '**PNR**' means a record of each passenger's travel requirements which contains information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey booked by or on behalf of any person, whether it is contained in reservation systems, departure control systems used to check passengers onto flights, or equivalent systems providing the same functionalities.
>
> (Article 3(5))

An annex to the directive (Annex I) lists the specific categories of PNR data that airlines ("air carriers") must send ("push": see Articles 3(7) and 8(1) and Recital 16) to the database of the PIU of the Member State on the territory of which the flight will land or from the territory of which the flight will depart (Art. 8(1)). This obligation is stipulated with regard to extra-EU

flights but can be extended by each Member State to apply also to intra-EU flights (Art. 2)[96] – and all but one Member States have done so.[97] If an airline sends "*data other than those listed in Annex I*", the PIU must "*delete such data immediately and permanently upon receipt*" (Art. 6(1)). The evaluation of the Dutch PNR Law gives as an example data on travel other than by airplane, such as travel by bus or train, that are sometimes included in PNRs,[98] and notes that it is unclear how or whether such excessive data are actually deleted.[99] Moreover, as we shall see below, the list in Annex I contains an open field – which makes it difficult to determine, at least in that regard, when data are "*data other than those listed in Annex I*".

The list of data in Annex I to the PNR Directive is considerably longer than the list of "advance passenger information" (API) listed in Article 3 of the API Directive. Below, I set out the data listed in Annex I to the PNR Directive and in Article 3 of the API Directive, showing the overlaps between them and the significant additional data set out in the former.

Annex I to the PNR Directive:	**Article 3 API Directive:**
1. PNR record locator [ref. nr.]	-
2. Date of reservation/issue of ticket	-
3. Date(s) of intended travel	[API data must be sent by the end of check-in]
4. Name(s)	Full names
5.Address and contact information (telephone number, e-mail address)	-
6.All forms of payment information, including billing address	-
7.Complete travel itinerary for specific PNR	[Only] Initial point of embarkation
8. Frequent flyer information	-
9. Travel agency/travel agent	-
10.Travel status of passenger, including confirmations, check-in status, no-show or go-show information	-
11. Split/divided PNR information	-

96 '**extra-EU flight**' means any scheduled or non-scheduled flight by an air carrier flying from a third country and planned to land on the territory of a Member State or flying from the territory of a Member State and planned to land in a third country, including in both cases flights with any stop-overs in the territory of Member States or third countries;

'**intra-EU flight**' means any scheduled or non-scheduled flight by an air carrier flying from the territory of a Member State and planned to land on the territory of one or more of the other Member States, without any stop-overs in the territory of a third country.

97 Staff working document (footnote 5, above), p. 24

98 Evaluation of the Dutch PNR Law (footnote 6, above), p. 101.

99 *Idem*, p. 102.

12. 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 [agent]; and - arrival agent * indents added	API data includes the following data also on minors: - full names; - date of birth - - - - - - - - - - - -
13. Ticketing field information, including ticket number, date of ticket issuance and one-way tickets, automated ticket fare quote fields	-
14. Seat number and other seat information	-
15. Code share information	-
16. All baggage information	-
17. Number and other names of travellers on the PNR	-
18. Any advance passenger information (API) data collected including:* - the type, number, country of issuance and expiry date of any identity document; - nationality; - family name; - given name; - gender; - date of birth; - airline; - flight number; - departure date; - arrival date; - departure [air]port; - arrival [air]port	Article 3 of the API Directive lists the following data: - the number and type of travel document used; - nationality; - full names} - full names} - - - date of birth; - } code of transport - } (i.e., airline code and flight nr.) - departure time } these presumably - arrival time } also show the date - } these are presumably also clear - } from the sending of the API data

- departure time; and - arrival time * Indents added	- departure time - arrival time Also: - the border crossing point of entry into the territory of the Member States (= arrival [air]port?) - total number of passengers carried on that transport (i.e., on the flight in question)
19. All historical changes to the PNR listed in numbers 1 to 18.	-

As can be seen from the lists, most of the data in both lists are relatively straight-forward, relatively "hard" data that can be useful in matching a PNR record against a list of "known" people, such as a list of formally wanted persons.

However, there is still a crucial distinction between the matching of such relatively "hard" basic identity data in lists (which, if the data are complete and reliable, will lead to a relatively high likelihood that a "match" really confirms that the person on one list is the same person as the person with the same details on the other list),[100] and matching of much "softer" data in a list against the same "soft" data in another list, i.e., where the latter data indicate no more than a probability. For instance, the fact that passenger John Bloggs is the convicted criminal John Bloggs may be reasonably assumed (where necessary, pending further examination) if the identity data in the relevant PNR (typically full name, date of birth, nationality) match those on a reliable list of convicted criminals. But the fact that passenger John Bloggs bought his ticket from a travel agent that in the past sold a ticket to a terrorist or serious criminal (a "suspicious" travel agent) proves very little. A match against "criteria" created by more sophisticated algorithms will be even less reliable. I will look at these issues further in the next sub-section (sub-section 4.9) and in section 5, sub-section 5.2(c). There, I will also discuss the fact that there will often be a double "match" of data received by at least some authorities in a Member State: a "match" against API data and a "match" (a confirmed "hit") against PNR data.

I should also note that in the PNR list there is one field in particular that is open-ended. This is Field 12 that asks for "*all available information on unaccompanied minors under 18 years*" entered into the "general remarks" field in airline PNR records.[101] It gives as examples ("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 agent; and arrival agent. However, those

[100] If the data are incomplete and not reliable, that will of course undermine the reliability of the match – or even make it impossible to declare whether there is one. Unfortunately, this is often the case with PNR data, as noted in sub-section 4.9(a), below.

[101] Field 18 also appears to be open-ended in that it uses the term "including". However, since it only applies to API data, it cannot be used for the collection of any data other than the API data set out in Article 3 of the API Directive, listed in the column next to that field.

are only examples. Airlines often put all kinds of other information in the "general remarks" field (and not only in relation to minors), such as information on meal preferences (e.g., vegetarian, gluten-free, or kosher or halal) or requests for a wheelchair, etc., that can indicate the person's health or religion.

(b) The use of sensitive data

According to Article 13(4):

> 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.

This list is close to but not quite identical to the list of "sensitive data" in Article 9(1) of the General Data Protection Regulation (GDPR) that, that article stipulates, should not be processed unless one of the exceptions in Article 9(2) applies.[102] Is there a difference between a person's "race" and his or her "racial origin"? Perhaps more importantly, is there a difference between a person's "religion" and his or her "religious beliefs"? And between "data revealing a person's health" and "data concerning health"?

I assume that any data that in any way strongly suggests any such matters are subject to the prohibition and must be immediately deleted upon receipt (and not used by the PIU). However, it would appear that sensitive data can still slip into the system. The report on the evaluation of the Dutch PNR Law gives as an example the email addresses of persons working for a political party, a trade union or a religious organisation (e.g.: John.Bloggs@AnarchistsUnited.eu, ThePope@RomanCatholicChurch.it).[103] It says that this problem is "recognised" and the authorities are "working on a solution" – but in the meantime, sensitive data can clearly still enter into the data processed by the Dutch PIU and are not always deleted.

Article 7(6) of the PNR Directive stipulates *inter alia* that:

> The 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 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.

I will discuss this stipulation (and the more general prohibition on discrimination in the EU Charter of Fundamental Rights and in international human rights law generally) in the next sub-section, on the different kinds of matches that are undertaken by the PIUs. There, I will both note (in sub-sections 4.9(d)) that PNR data can also be matched against national lists and data "repositories" that may well contain sensitive data, and more specifically (in sub-section 4.9(f), at (fe)) that the provisions in the PNR Directive do not really protect against discriminatory outcomes of the profiling that it encourages.

---

102 "*Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.*"

103 Evaluation of the Dutch PNR Law (footnote 6, above), p. 102. The (made up) examples are my own.

4.9 The different kinds of matches

Article 6(2) and (3) list the (only) three purposes for which PNR data may be processed by the PIUs in a rather confusing way, as follows:

> **(2) The PIU shall process PNR data only for the following purposes:**
>
> (a) carrying out an assessment of passengers prior to their scheduled arrival in or departure from the Member State to identify persons who require further examination by the competent authorities referred to in Article 7, and, where relevant, by Europol in accordance with Article 10, in view of the fact that such persons may be involved in a terrorist offence or serious crime;
>
> (b) responding, 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, and to provide the competent authorities or, where appropriate, Europol with the results of such processing; and
>
> (c) analysing PNR data 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.
>
> **(3) When carrying out the assessment referred to in point (a) of paragraph (2), the PIU may:**
>
> (a) compare PNR data against databases relevant for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, including databases on persons or objects sought or under alert, in accordance with Union, international and national rules applicable to such databases; or
>
> (b) process PNR data against pre-determined criteria.

This is confusing because it mixes up a number of very different kinds of checks, of matching and analysing of the data, that all appear to be envisaged in (or at least allowed under) the directive (even if they may not all be yet in actual use in all Member States)**:** the matching of basic identity data in PNRs against the same identity data in lists of already "known" formally wanted persons or already listed "persons of interest"; the matching of PNR data against other relatively "hard" data, such as data on lost/stolen/fake credit cards or lost/stolen/fake identity or travel documents; the matching of data in PNRs against less determinative data such as the use of a "suspicious" travel agent or a "suspicious" travel route; and the matching of PNR data against more sophisticated abstract patterns and profiles, in order to "*identify*" individuals as *possibly* being involved in terrorism or other serious crimes.[104]

Crucially, as the quotation marks above indicate, the latter form of "identifying" is rather different from the former ones.[105] In case of the first use – identifying "known" formally wanted criminals or other "known" persons (including previously already "known" "*subjects of interest*" or "*persons … [targeted] for discreet checks, inquiry checks or specific checks*")[106]

---

104 There are some overlaps between these categories, as I will note in the sub-sections.

105 I draw on a more elaborate discussion of this difference in: Douwe Korff & Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards (footnote 17, above), pp. 32 – 34.

106 See section 3.7, above.

from lists of such persons – the term means "*confirming that a certain person is a specific person named (or otherwise identified) on a list or official record or document*". (However, identifying a person on a list of formally wanted persons is of course still different from identifying a person who is listed as merely "*of interest*"; they have different consequences and implications, as discussed in sub-section 4.14 and section 5, below.)

By contrast, pro-active "identification" of an individual (or an individual's actions) as matching certain pre-determined criteria (be these simple or complex) merely indicates a certain probability (which can be quite low) that the person "*may*" fall into a pre-defined category (i.e., fits the pre-determined set of criteria). As noted in the Korff/Georges paper on which I draw (slightly edited):[107]

> This semantic difference has seriously hampered the debates on PNR (and on other big data sets). The authorities repeatedly assert that these systems are only used "to identify terrorists" (and/or similar bad people); and most members of the public – and indeed many in positions of authority, such as members of parliament or judges – will understand this term to refer to "identification" in the first sense mentioned above. But in reality it is increasingly used in the second sense.
>
> Any honest, transparent debate about the uses of PNR data or other big datasets should be completely clear about the way in which the terms are used. Unfortunately, this is not yet the case.

In recognition of the above, in the next six sub-sections I discuss separately:[108]

- the matching of relatively "hard"[109] basic identity data in PNRs against SIS alerts relating to "known" formally wanted persons and similar alerts or data in national lists in the "confirming of identity" sense (sub-section (a));

---

[107] Douwe Korff & Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards (footnote 17, above), pp. 34.

[108] The distinctions made in the indents partly correspond to the **three elements of the UK's bulk interception of electronic communications programme**, as described in the UK ISC report (footnote 94, above):

- identifying and monitoring of individuals "known" to pose a threat by means of what are referred to in the UK as "**simple selectors**";
- "identifying" new threats through more sophisticated data mining (i.e., the creation of "intelligence" based on "patterns" and "profiles"); and
- "identifying" previously unknown "persons of interest" through matches against those "patterns" and "profiles" (i.e., through what are referred to in the UK as "**complex selectors**" and "**selection rules**").

See *Part Two* of the submission by Ian Brown and me to European Union bodies on The inadequacy of UK data protection law in general and in view of UK surveillance laws on *UK surveillance law* (footnote 52, above).
These different kinds of checks, matches and analyses also basically correspond to those noted by the EDPS in his first opinion on the proposal for the PNR Directive (footnote 77, above), quoted in sub-section 4.3, above: "*to identify known terrorists or known criminals involved in organised crime, by comparing their names with those included in lists managed by law enforcement authorities*"; "*to gather intelligence with regard to terrorism or organised crime*", and more precisely "*to carry out risk assessment of persons, obtain intelligence and make association between known and unknown people*" on the basis of "*patterns*" and "*profiles*".

[109] There is no absolute line between "hard" and "soft" data: a relatively "hard" fact such as a name still only indicates a probability of a match, especially for common names. But there is still a fundamental distinction between trying to match relatively "hard" data on an air passenger against lists of the same categories of data and trying to match a range of data on a passenger against "patterns" or "profiles".

- the matching of relatively "hard" basic identity data in PNRs against SIS alerts relating to "known" "persons of interest" and similar alerts in national lists in the "confirming of identity" sense (sub-section (b));
- the matching of PNR data against relatively "hard" data on lost/stolen/fake credit cards and lost/stolen/fake identity or travel documents (sub-section (c));
- the matching of PNR data against other, unspecified, supposedly relevant (in particular national) databases (sub-section (d));
- the matching of PNR data against lists of "suspicious travel agents", "suspicious routes", etc. (sub-section (e)); and
- the matching of PNR data (and other data?) against more complex "pre-determined criteria" or profiles[110] (sub-section (f)).

The differences between these checks have implications in relation to what kinds of "hits" should be regarded as "positive" results under the PNR Directive, as indicated in these sub-sections. I will discuss the implications in section 5.

(a) Matching of basic identity data in PNRs against the identity data of "known" formally wanted persons

As explained in the staff working document:[111]

> According to Article 6.3(a) of the PNR Directive, when pre-screening passengers prior to their arrival or departure, the Passenger Information Unit may compare PNR data against databases relevant for the purposes of fighting terrorism and serious crime 'including databases on persons or objects sought or under alert'. The SIS, the most widely used and largest information sharing system for security and border management in Europe, is clearly one of such databases.

PNR data are also checked against "**national law enforcement repositories**" – presumably, similar lists of "known" formally wanted persons and, perhaps, "known" "persons of interest", as identified in the relevant Member State and regulated in national law.[112] In the remainder of this sub-section, I will focus on the SIS alert categories, with somewhat looser references to "similar data" or "similar alerts" in these "national law enforcement repositories" (of which no details are provided in the staff working document).

---

110 In UK intelligence terminology referred to as matching against "complex selectors". See footnote 108, above.

111 Staff working document (footnote 5, above), section 6.4, on p. 29. On SIS, see section 2, sub-section 2.3, above. Note that not all PIUs check against (all) SIS alerts. The Dutch PIU (Pi-NL), for example, only checks against "Article 26 alerts" (alerts for persons wanted for arrest for extradition) and "Article 36 alerts" (alerts relating to people or vehicles requiring discreet checks). Evaluation of the Dutch PNR law (footnote 6, above), p. 77.

112 Staff working document (footnote 5, above), p. 30. I will discuss the possibility of PNR data being checked against more abstract "criteria" in such "repositories" and as created by Europol in sub-section (f).

As already noted in sub-section 4.2, above, and in accordance with Article 6(5), the PIU checks generally consist of **two-steps** – which is of particular importance in relation to basic identification checks.[113]

In principle, the matching of basic identity data from PNRs against lists of basic identity data of actual or suspected "known", listed terrorists or serious criminals (or indeed of the much less well-defined category of "known", listed "persons of interest": see sub-section (b) below) **should be fairly straight-forward**, especially if both are in (compatible) electronic format: much of this can be done – and it would appear is done – by automated means. If this results in an **initial "hit",** the match is **checked manually**. Only **"confirmed hits"** are passed on to the competent authorities "for further examination".

In relation to basic identity checks, it appears that if it is confirmed that the identity data of a passenger match the identity data of a "known" formally wanted person on whom there is a SIS alert or if those data match the identity data of a "known" person on a comparable "national law enforcement repository", then that match is regarded as a "*fact*" that shows "*that [that] person[ ] may be involved in a terrorist offence or serious crime*", and should be "further examined" by the relevant competent authorities (and/or Europol) in relation to PNR-relevant offences. **However, there are some serious issues with this.**

First of all, on the one hand, **the quality of the PNR data as received by the PIUs, including even of the basic identity data, is apparently terrible and "often limited":**[114]

> **Reliability of PNR data**
>
> PNR data are generally provided by the passengers themselves. In accordance with Article 8 of the Directive, air carriers are obliged to transmit PNR data to the extent that they have already collected such data in the normal course of their business. Accordingly, air carriers are not obliged to ensure that the data transmitted to the authorities are complete, accurate and up-to-date. Under the PNR Directive, carriers can only be sanctioned for failing to transmit the PNR data they have or for not doing so in the right format (Article 14). **National authorities have identified issues arising from the poor quality and incompleteness of PNR data as the main challenge preventing them from using PNR data to its full potential.** However, air carriers argue that concepts such as 'quality' and 'completeness' should not be applicable to PNR given its declaratory and unverified nature.
>
> When speaking of data quality, law enforcement authorities usually refer to issues such as spelling mistakes, data elements being misplaced in the PNR message (e.g. the email address is contained in the field for payment details) and the fact that in some cases abbreviations such as Mr are attached to passengers' surnames, among others. These **seemingly minor details may have a significant impact on the automated processing of PNR data: the data received by the Passenger Information Unit may be unreadable to the IT system or require additional maintenance and adaptations.** At the same time, air carriers do not have any obligation to verify this kind of issues before transferring PNR data.

---

113 I will explain why the second step, the manual review, is less relevant in the other checks in the sub-sections on those other checks, below.

114 Staff working document (footnote 5, above), section 6.1, on p. 27. The words "often limited" are from section 6.4, on p. 30.

> As regards completeness, air carriers have further underlined that the amount of data collected are determined by commercial considerations. The reservation data collected can be very limited, in some cases including only the name and the surname of the passenger, combined with the basic information about the flight (date, itinerary). In turn, national authorities point out that **the lack of certain data allowing to confirm the passengers' identity impairs the efficient use of PNR data and constitutes a key challenge for the Passenger Information Unit staff in their daily work.**
>
> Notably, without the date of birth it may be impossible to confirm the identity of the person, particularly for passengers with common names. This may hinder the possibility to compare PNR data against certain databases relevant for the fight against terrorism and serious crime – including the SIS – which require the use of more complete data for a person to carry out a meaningful search. For example, **one Member State reported that a large majority of matches have to be discarded as the manual intervention needed to confirm the result of automated processing would be too cumbersome, and ultimately impossible, in the absence of additional elements necessary to confirm the identity of the passenger.**

It is not clear what level of uncertainty or missing data leads to the discarding of the initial "hit", and what level could be regarded by a PIU as not standing in the way of passing on the "hit"; practice may will differ between different PIUs. It is also not made clear in the staff working document (or anywhere else I have been able to look) whether the absence of a basic datum such as a date of birth can be "compensated" for by a match with another element, such as the use of a "suspicious" travel agent, or of a "suspicious" travel route, or of a "suspicious" amount of luggage. If there is guidance on this, it is not made publicly available.

All we know is that the vast majority of initial "hits" are discarded:[115]

> **[T]he statistics gathered by the Commission for 2019 indicate that 0.59% of all passengers whose data have been collected have been identified through automated processing as requiring further examination. An even smaller fraction of 0.11% was transmitted to competent authorities.***

* Note that, contrary to what the Commission staff document asserts, the 0.11% does not relate to "*a very limited number of passengers*".[116] Rather, given that the PIUs process about 1 billion PNRs on what I believe to be approximately 500 million individuals, the data on about 500,000 individuals are passed on annually for "further examination" by law enforcement and national intelligence/state security agencies. To call that "*a very limited number*" is simply dishonest. Moreover, as the evaluation of the Dutch PNR Law rightly notes, for innocent air travellers the passing on of their data for "further examination" by law enforcement (and intelligence) agencies constitutes a serious, unwarranted interference with their rights.[117] I discuss this further in sub-section 4.14 on *the consequences of a "match"* and in section 5 on *the suitability, effectiveness and proportionality of the checks*.

Given that the manual review is less relevant in the other checks (as discussed in the sub-sections on those checks, below), **it may be assumed that the vast majority of the 81% of**

115 *Idem*, section 5.1, on p. 18.

116 *Idem*.

117 "*[V]anuit het zicht van de bonafide reizigers van wie de gegevens ten onrechte als match aan de Frontoffice zijn verstrekt, is dat wel ingrijpend.*" Evaluation of the Dutch PNR Law (footnote 6 , above), p. 78.

initial "hits" that were not passed on to competent authorities[118] were the result of insufficient or insufficiently verifiable basic identity data in the PNRs. In other words, the PNR data are indeed often "too limited" to serve the purpose of allowing basic identity checks.

Note: According to the report on the evaluation of the Dutch PNR Law, the Dutch PIU (Pi-NL) received PNR data on some 36 million passengers in part of 2019, and on 24 million passengers in 2020 (the number of passengers in that year is much lower because of the Covid pandemic).[119] There were, in that country, in both 2019 and 2020 (the two years covered), initial "hits" in relation to 0.31% of all the passengers on whom PNR data had been received,[120] and about 80% of these – i.e., "hits" on about 0.25% of all passengers – were confirmed by the *Frontoffice* and passed on to (other) competent authorities as "alerts".[121] In other words, in the Netherlands only about 20% of initial "hits" are not passed on to competent authorities. This is presumably because the *Frontoffice* checks the initial "hits" against various police databases (something that the Dutch PIU itself is not allowed to do). (The *Frontoffice* also then "enriches" the (PNR) data from the initial "hits" with information from those police databases, such as a photograph, warnings about the person such as "[may be] armed" or "violent" (categories allowed in SIS), and "other information from the (police)databases [*(politie)systemen*) relevant to the competent authorities" to which the "alert" is sent.)[122]

However, secondly and seemingly paradoxically, **most of the long lists of PNR data are not needed for basic identity checks**: full names, date of birth, gender and citizenship/nationality should suffice – and a passport or identity card number would make the match more reliable still. All those data are included in the API data, and all are included in optical character recognition format in the machine-readable travel documents (MRTD) that have been in wide use since the 1980s.[123] As it is put in the staff working document:[124]

> API data are basic information about passengers and crewmembers. It includes elements such as the name, date of birth, gender, citizenship, and travel document data (e.g. passport number). This information is usually available from the machine-readable zone of travel documents.

Under the API Directive, API data must be provided by airlines in relation to all extra-EU flights, but not in relation to intra-EU flights.[125] The staff working document repeatedly suggests that the non-availability of date of birth information in particular is a significant problem in relation to PNRs, more in particular in relation to intra-Schengen flights and in relation to SIS checks:[126]

> [I]nformation on the passenger's date of birth is usually lacking in intra-Schengen flights where airlines are not required to collect API. This affects the ability of Member States to query PNR data against the SIS – as the date of birth is required to perform exact

---

118 The part of initial "hits" that are confirmed and passed on is 11/59=0.19 (=19%). The part of initial "hits" that are not passed on is 48/59=0.81 (=81%).

119 Evaluation of the Dutch PNR Law (footnote 6, above), p. 9

120 *Idem*, p. 76.

121 *Idem*, p. 78. On the terminology and the in-between body, *Frontoffice*, see footnote 66, above.

122 *Idem*, p. 77.

123 See: https://en.wikipedia.org/wiki/Machine-readable_passport

124 Staff working document (footnote 5, above), section 6.1, on p. 27.

125 See footnote 96, above.

126 Staff working document (footnote 5, above), section 6.4, on p. 30.

> matches – and creates uncertainty as to whether any positive results obtained in the pre-screening process indeed concern a person subject to an alert in the SIS.

In other words, paradoxically, PNR data are both excessive for the purpose of basic identity checks (by containing extensive data that are not needed for such checks), and insufficient ("too limited"), in particular in relation to intra-Schengen flights (by not [always] including the dates of birth of the passengers).

The researchers carrying out the evaluation of the Dutch PNR Law noted that in relation to extra-EU flights, matches against the API data held by the API Centre of the Dutch *gendarmerie* (KMar) overlapped with the matches (confirmed "hits") against the PNR data that were passed on to the *gendarmerie* by the Dutch PIU, resulting in matches on the same person being twice checked against SIS alerts. An earlier assessment indicated that about 30% of the PNR "hits" that were confirmed by the Dutch PIU had already been noted as a match with the API data.[127] This raises yet further questions about the disproportionality of the use of PNR data.

There is a further, third issue. This is that (as already noted at 2.2, 4.6 and 4.7, above), the lists against which the PNR data are compared, including in particular the SIS alerts and the EAW lists, relate to many more crimes than are subject to the PNR Directive ("**PNR-relevant offences**") – which specifically states in Article 1(2) 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 [as defined under the directive][128] … (emphasis added)

This poses a **dilemma** for the PIUs and the Member States, discussed in the staff working document as follows:[129]

> Another important issue concerns the broader scope of the SIS, compared to the PNR Directive, combined with the lack of sufficient detail concerning the type of offence underpinning a specific SIS alert. **This raises the risk of the Passenger Information Unit obtaining matches that are not 'PNR-relevant' when performing database checks.** Again, the manual review process, while offering the opportunity to dismiss any non-PNR related matches, is time and resource-intensive. **Ignoring potential hits also raises complex legal questions, as the authorities usually have the duty to act when confronted with a possible criminal offence, irrespective of whether this fits the strict purpose limitation requirements of the PNR Directive.**
>
> *In practical terms, Member States have tackled these challenges in different ways. Some of them refrain from comparing PNR data against the SIS and limit such comparisons to national law enforcement repositories and pre-determined criteria. Others run PNR data queries only against specific SIS alerts, notably those under Articles 26 and Article 36.2 and 36.3 of Council Decision 2007/533/JHA. While these approaches help limit the number of 'false positives'/ non-PNR related matches, they may also lead the authorities*

---

127 Evaluation of the Dutch PNR Law (footnote 6, above), p. 80. The earlier assessment, carried out in 2020, is known as the Ketenbrede Impact Assessment – but this was not a data protection impact assessment, but sought to assess the impact of the application of the law on the workload of the various authorities.

128 See section 4.6, above, and Attachment 1.

129 *Idem*. The document notes that this issue is likely to grow in future:

> *to miss potentially relevant information. For this reason, other Member States compare PNR data against all alert categories and rely on the manual validation step to filter out matches that do not specifically relate to the purposes of the PNR Directive, which in turn leads to the aforementioned efficiency issues, and raises questions as to whether these broad comparisons are fully aligned with the Directive's strict purpose limitation.*
>
> (emphases, italics and paragraph break added)

The staff working document notes that this issue may become even more problematic in future:[130]

> In the future, new challenges may emerge from the interaction between PNR and other instruments in the travel intelligence landscape, such as the European Travel Information and Authorisation System (ETIAS) and the Entry/Exit System (EES). Aspects that will warrant further examination concern, for example, the relationship between the Passenger Information Units and the ETIAS National Units in the Member States, and the way to ensure that all available travel information (in particular API, PNR and ETIAS related) is used in the most effective manner.

The staff working document actually understates the issue when it says this "*raises questions as to whether these broad comparisons are fully aligned with the Directive's strict purpose limitation*". **Put more directly: those "broad comparisons" of PNR data with lists relating (also) to "not PNR-relevant crimes" are manifestly incompatible with "the Directive's strict purpose limitation" principle.** Even the checks against SIS alerts under Articles 26 and Article 36(2) and (3) of Council Decision 2007/533/JHA clearly go beyond the scope of the PNR Directive.[131]

It would therefore appear that only a few ("some") EU Member States, i.e., those that actually do not match the PNR data against the SIS alerts at all, act in compliance with the directive. Or to put it more starkly: *the vast majority of the EU Member States do not respect the purpose limitation principle on which the PNR Directive is supposed to rest.*

Finally, fourth, the staff working document claims that in relation to situations in which the PNR data is "too limited" (typically, by not including date of birth):

> The individual manual review provided for in Article 6.5 of the PNR Directive protects individuals against the adverse impact of potential 'false positives' ...

This is simply untrue, also in relation to confirmed identity checks. In particular, confirmed "hits" against SIS alerts and EAWs (or similar national law enforcement repositories) relating to "not PNR-relevant" offences should of course not be considered as positives (let alone true positives) in terms of that directive – and it is clear from the staff working document that not all Member States remove initial "hits" of this kind and do not pass them on for further examination to their competent authorities; indeed, in certain countries, in which authorities have a legal duty to not ignore any crimes that "come to their attention", they will be obliged

130 *Idem*.

131 Article 26 of Council Decision 2007/533/JHA covers "persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes" – but EAWs can relate to clearly not PNR-relevant crimes. Article 36(2) and (3) relate to alerts on persons and objects for discreet checks or specific checks (and presumably inquiry checks) – which are also not limited to PNR-relevant crimes.

to pass such "hits" on even if that is in breach of the PNR Directive purpose limitation principle.

In my opinion, while a confirmed matching of identity data in relation to a person who is formally wanted in relation to (formally suspected of, charged with, or convicted of) PNR-relevant offences can be regarded as a "positive" result of the identity check, *a "hit" in relation to a person who is wanted for non-PNR-relevant offences should of course not be regarded as a positive result under the PNR Directive* (see also section 5, sub-section 5.2(a), at (ab), below). Yet in at least a number of Member States, these results are not removed, but still passed on "for further examination".

(b) Matching of basic identity data in PNRs against the identity data of "known" "persons of interest"

In principle, the matching of basic identity data from PNRs against lists of basic identity data of "persons of interest" listed in the SIS system (and comparable categories in national law enforcement repositories), like the matching of data on formally wanted persons, **should be fairly straight-forward**.

However, the PNRs in this regard first of all suffer from the same two deficiencies as were discussed in relation to matches for formally wanted persons, discussed at (a), above: PNR data are both excessive for the purpose of basic identity checks (by containing extensive data that are not needed for such checks), and insufficient ("too limited"), in particular in relation to intra-Schengen flights (by not [always] including the dates of birth of the passengers).

The third issue identified in the previous sub-section, that SIS alerts (and similar alerts in national law enforcement repositories) can relate to many more criminal offences than those that are "PNR-relevant" also applies: many persons labelled "person of interest" will be so labelled in relation to "not-PNR-relevant" offences.

However, in this context, the issue is even worse. In its *DRI* judgment, the CJEU criticised the fact that the Data Retention Directive:

> affect[ed], in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. (para. 58)

The matching of data on "known" formally wanted persons can at least be said to affect only persons who are in "*a situation which is liable to give rise to criminal prosecutions*" (or where such prosecutions have even already commenced). By contrast, in relation to persons labelled "persons of interest" there will often be "*no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime*" – or at least, any such link would not need to imply any possible culpability (e.g., when witnesses or victims are so labelled).

In my opinion, while a confirmed matching of identity data in relation to persons who are formally wanted in relation to (formally suspected of, charged with, or convicted of) PNR-relevant offences can be regarded as a "positive" result of an identity check, *a "hit" in relation to persons who are labelled "person of interest" should not be regarded as a positive result under the PNR Directive – certainly of course not if they are so labelled in relation to non-PNR-relevant offences, but also not if they are in no way implicated as in any way being culpable of PNR-relevant offences.*

In my opinion, *even confirmed "hits" confirming the identity of already listed "persons of interest" should not be regarded as "positive" results under the PNR Directive unless they result in those persons subsequently being formally declared to be formal suspects in relation to terrorist or other serious, PNR-relevant criminal offences*.

(See again further section 5, sub-section 5.2(a), at (ab), below)

There is one final issue in this regard. This is that while **PIU staff** can note deficiencies in basic identity data, and decide not to confirm a "hit" on that basis (as discussed above, at (a)), they **are not in a position to check whether a person is rightly or wrongly labelled a "person of interest"**; in fact they may have no idea as to why a person is so labelled at all (frontline police officers etc. are not provided with this information).

It may therefore be assumed that whereas PIU staff may decide not to pass on a "hit" on a "person of interest" because the identity data are insufficient, in effect that will be the only reason to not confirm and pass on the "hit".

(c) Matching of PNR Data against data on lost/stolen/fake credit cards and lost/stolen/fake identity or travel documents

The staff working document makes clear that PNR data are checked by "a large majority of PIUs" against **Interpol's Stolen and Lost Travel Document database** as one "relevant database".[132] However, this is somewhat of a residual check because that database is also already made available to airlines through Interpol's "**I-Checkit**" facility:[133]

> Criminal groups and terrorists use stolen travel documents to conceal their identities and cross borders undetected. Given this threat, and faced with increasing volumes of international passengers, countries need to heighten their border control and identity management measures.
>
> I-Checkit is a screening solution that complements and enhances national border security systems. It allows trusted partners in the private sector to conduct advanced passenger checks in real-time, in collaboration with the law enforcement community.
> …
>
> I-Checkit enables carriers to submit travel document information for screening against SLTD database (travel and identity documents). The data screened does not include names of individuals.

---

132 Staff working document (footnote 5, above), section 3.5, on p. 8.

133 See Interpol, *I-Checkit*, at: https://www.interpol.int/How-we-work/Border-management/I-Checkit

> A database match triggers an instant alert so the situation can be investigated. Notifications are sent to INTERPOL's General Secretariat and to National Central Bureaus in the countries concerned, and other relevant national law enforcement entities. In some cases, the carrier's security teams can also receive the notification so they can out a secondary check of the document in question at the boarding gate.

At least in relation to extra-EU flights, many people trying to use stolen travel documents will presumably already be refused boarding (or even have their attempt to book a flight refused) by the airlines on the basis of such a match.

Interpol wants to expand I-Checkit to other areas, including the financial sector.[134] Presumably, in the meantime, lost, stolen or fake credit cards are listed mainly in national "repositories" – but again, in most cases lost or stolen cards, once reported, will have been cancelled by the banks concerned and quickly become unusable to any malignant finder or thief.

Still, apparently, there are still some (many?) lost/stolen/fake credit cards and lost/stolen/fake identity or travel documents that slip through these checks, and some of those may well be used by terrorists and other serious criminals, also for air travel. However, they may of course also be used by criminals involved in non-PNR-relevant (lesser) crimes – which raises the same dilemma about purpose-limitation as discussed at (a) and (b), above.

Moreover:

Even leaving the issue of purpose-limitation aside, *a "hit" against a listed lost/stolen/fake credit card or a lost/stolen/fake identity or travel document should still only be considered a "positive result" in terms of the PNR Directive if it results in a person subsequently being formally declared to be (at least) a formal suspect in relation to terrorist or other serious, PNR-relevant criminal offences* (see again section 5, sub-section 5.2(a), at (ab), below).

(d) Matching of PNR data against other, unspecified, supposedly relevant (in particular national) databases

It is far from clear what databases can be – and in practice, in the different Member States, what databases actually are – regarded as "relevant databases" in terms of the PNR Directive. As already noted, the staff working document mentions "*for example, the Schengen Information System (SIS) or national watch lists*".[135] But those are of course only examples.

At the July 2021 Court hearing, there were some exchanges on what kinds of data collections PNR data could be matched against. The representatives of some Member States (France and Germany) indicated that their PIUs were only authorised to match the PNR data they receive against national lists of wanted people or things. It was not made clear whether these lists also include lists of "*subjects of interest*" or "*persons … [targeted] for discreet or specific checks*" (or whatever the French and German equivalents are).

But the Commission indicated that Member States could authorise matching also against **other "relevant" databases**. The Judge-Rapporteur asked whether this could include matches

134 *Idem*.

135 Staff working document (footnote 5, above), p. 7.

against, e.g., *Facebook*, or *Amazon* or *Visa*, or against databases with telecommunications data. The representative of the Commission said that the data of *Facebook*, *Amazon* and *Google* could not be regarded as "relevant", and that law enforcement databases (*des bases policières*) would be the most obvious "relevant" databases. But the Commission did not exclude matches against other databases, such as databases with financial data (credit card data?) or telecommunications data (location data?).

Given that the list of PNR data expressly also asks for (among many other items) telephone numbers (presumably including mobile phone numbers), e-mail addresses and "all forms of payment information, including billing address", it would appear clear that the text of the directive does not prohibit matching of PNR data against the databases of e-communication service providers, banks and payment system providers (to the extent that such data are available to the authorities). Indeed, there is little point in including those data if they are not used in this way (in some way).

Recital (15) of the PNR Directive stipulates that:

> 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.

One may question whether the data elements listed in Annex I to the directive (reproduced in sub-section 4.8, above) really all constitute such "*details …. enabling … the authorities to identify passengers representing a threat to national security*" – or if they do, what data would not constitute such details. But apart from that, the possibility of matching PNR data against other data in essentially unspecified other databases also makes a mockery of this stipulation: the data in such other databases are not "PNR data", but they are still used in the searches.

In any case, as already noted in section 2, sub-section 2.2, above, in advanced, sophisticated data mining (as applied to PNR data, as discussed in sub-section 4.9(f), below), the data to be analysed are not limited to what can be *a priori* regarded as relevant data; rather, the aim is "*to discover the hidden pattern, the unexpected correlation*" in essentially any large dataset including (especially) data that one would not have thought in advance to be relevant.

From the "case studies" provided in the staff working document (discussed in Attachment 2), it is clear that checks are certainly made against lists of travel agents from whom terrorists or other serious criminals have in the past obtained flight tickets (see below, at (e)). Presumably, law enforcement agencies also keep records of payment cards and mobile phones that in the past have been used by terrorists or other serious criminals (even if they were not lost or stolen). There may be other "hard" elements that are recorded in lists or data sets created by such agencies that are passed on to the PIUs. In the UK, such lists of relatively "hard" data are known as "**simple selectors**".[136]

[136] See footnote 108, above.

Although practice may differ between Member States, nothing in the PNR Directive stands in the way of law enforcement agencies (and intelligence agencies) creating such lists; and under the PNR Directive, the PIUs are allowed to match the PNR data they receive against such lists as long as those lists are deemed "relevant".

In my opinion – and in the view of the EDPS: see below – such matching of more than basic "hard" data can be regarded as justified and legitimate in the context of a formal investigation against a person reasonably suspected of a (serious) criminal offence, subject to crucial safeguards such as a judicial investigation order. However, the checks by the PIUs are on hundreds of thousands of individuals who are not in any way suspected of any offence, and the vast majority of whom will never become formal suspects or charged with any offence.

This means that the criticism of the European Data Protection Supervisor in his first opinion on the then draft PNR Directive of March 2011 still stands:[137]

> [The provisions in the PNR Directive as then drafted] provide[ ] that a PIU may carry out an assessment of the passengers and in this activity may compare PNR data against "relevant databases" … . **This provision does not indicate which are the databases that are relevant. Therefore the measure is not predictable,**[138] **also a requirement under the Charter and the ECHR.** The provision moreover **raises the question of its compatibility with the purpose limitation principle**: according to the EDPS, it should be excluded for instance for a database such as Eurodac which has been developed for different purposes.[139] Besides, it should be possible only in case there is a specific need, in a particular case where there is a pre-existing suspicion on a person after a crime has been committed. Checking for instance the database of the Visa Information System[140] on a systematic basis against all PNR data would be excessive and disproportionate.

The vagueness of the phrase "relevant databases" in Article 6(3)(a) and the apparently wide discretion granted to Member States to allow matching against all sorts of unspecified data sets is incompatible with the Charter of Fundamental Rights and the European Convention on Human Rights. It means the application of the law is not clear or foreseeable to those affected – i.e., the provision is not "law" in the sense of the Charter and the Convention (and EU law generally) – and that the laws can be applied in a disproportionate manner.

---

137 EDPS, (First) Opinion of the Proposal for the PNR Directive (footnote 77, above), para. 18.

138 Or in ECHR terminology, foreseeable. See footnote 56, above.

139 4 The purpose of Eurodac "shall be to assist in determining which Member State is to be responsible pursuant to the Dublin Convention for examining an application for asylum lodged in a Member State, and otherwise to facilitate the application of the Dublin Convention under the conditions set out in this Regulation", according to Article 1 (1) of Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316, 15.12.2000, p . 1. [original footnote]

140 "The VIS shall have the purpose of improving the implementation of the common visa policy, consular cooperation and consultation between central visa authorities by facilitating the exchange of data between Member States on applications and on the decisions relating thereto", according to Article 2 of Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218, 13.8.2008, p. 60. [original footnote]

In other words, even in relation to the basic checks on the basis of lists of "simple selectors", the PNR Directive does not ensure that those checks are based on clear, precise, and in their application foreseeable Member State laws, or that those laws are only applied in a proportionate manner. In the terminology of the European Court of Human Rights, the directive does not protect individuals against arbitrary interferences with the rights to privacy and protection of personal data.

(e) Matching of PNR data against lists of "suspicious travel agents", "suspicious routes", etc.

The staff working document repeatedly refers to checks of PNR data against "patterns", and in that regard mentions specifically "travel behaviours":[141]

> Even more importantly [than "automatically checking of PNR data before arrival or departure against various law enforcement databases of persons and objects sought" (as discussed in sub-sections (a) – (c), above)], PNR data can be used **to identify persons involved in criminal or terrorist activities who are, as of yet, not known to the law enforcement authorities**. This is because **the processing of PNR data can highlight** – for a further assessment – **passengers whose travel behaviours are atypical or fit the travel patterns usually encountered in the case of offenders.** This objective can only be achieved through the use of PNR data. In practice, **this is done by comparing PNR data, through automated means, against combinations of predetermined fact-based risk indicators.**
>
> Examples of such risk-indicators reported by national authorities include ***the fact that the passengers have booked their tickets using travel agencies known to be used by traffickers*** or have chosen ***travel routes that are both longer and more expensive than the routes a person travelling for business or tourism purposes might have chosen***. The use of pre-determined criteria may also identify ***passengers whose luggage does not correspond with the length of the stay and destination***, which may raise suspicions of involvement in trafficking of illicit goods or money laundering. Similarly, information that ***a credit card belonging to a suspected trafficker*** was used in order to book a ticket for another person might reveal the existence of a form of trafficking, even though the person travelling may not be known to law enforcement authorities.
>
> According to the Member States, used in combination with other investigative tools and methods, PNR allows law enforcement authorities **to detect suspicious behaviour**, better target their investigation, prioritise one lead over the other, build up their case and gather evidence necessary to obtain a conviction.

A recent case from the Netherlands mentions the singling out (i.e., the "identifying" in terms of the PNR) of a person as a suspected money smuggler on the basis that the person was "dressed in a suit" and "walking fast" (and black):[142]

> Mpanzu Bamenga, a former Eindhoven city councillor ... was singled out for special questioning at passport control at Eindhoven airport after returning from Rome where

---

141 Staff working document (footnote 5, above), section 5.1, on pp. 15 – 16, emphases added.

142 *Border police to stop using ethnic profiling ahead of talks with MPs*, Dutch News, 19 November 2021, available at: https://www.dutchnews.nl/news/2021/11/border-police-to-stop-using-ethnic-profiling-ahead-of-talks-with-mps/

> he had attended a conference. Dressed in a suit, he was walking fast, other indicators, it later transpired, for resembling a 'Nigerian money smuggler'. In the statement, first obtained by the Volkskrant, the border police said from the perspective of both legitimacy and trust, it had decided 'not to let ethnicity be an indicator in profiles or selection decisions'.

As explained in the above report, the Dutch border police has since agreed "to stop using ethnic profiling", even though, astonishingly, a Dutch court had ruled that this "did not amount to discrimination". However, it does not appear to have given up on using the above kinds of flimsy patterns – walking fast in a suit?? – as a means to determine who "may be" involved in certain serious crimes.

The examples mentioned in the Commission staff working document are all of attempted matches of fairly straight-forward elements in PNRs against fairly straight-forward criteria: lists of "suspicious travel agents", "suspicious travel routes", or credit cards previously used for nefarious purposes – what in the UK are referred to as "simple selectors" (like lists of lost/stolen/fake credit cards or travel documents). They are exactly the kinds of elements mooted for "terrorist profiles" in the early 2000s, as noted in section 2, sub-section 2.1, above. As also noted there, in sub-section 2.2, practice has since moved towards more complex data mining – which I will discuss in the next sub-section – but here, it is worth first still noting these simpler ones.

The point to be made in that respect is that a "hit" in relation to the relatively simple "suspicious" elements is far from conclusive in proving, or even reasonably indicating, that the person to whom the "suspicious" pattern relates is actually in any way involved in crime – any crime, let alone terrorism or serious crime. Travel agents who in the past have sold air travel tickets to terrorists or other serious criminals will also have sold (many) tickets to entirely innocent travellers – even if they sold the tickets to the terrorists knowingly (which they may not have done). There may well be "*travel routes that are both longer and more expensive than the routes a person travelling for business or tourism purposes might [normally] have chosen*" – but that still does not mean that all people taking the "suspicious" route should be regarded as, or even treated as likely or possibly to be, a terrorist or serious criminal. Not all travellers with "unusual" amounts of luggage will be terrorists, money launderers or other serious criminals.

No proper prosecuting or judicial authority could declare travellers to be a formal suspect – let alone to charge, prosecute or convict a traveller – on the basis of a match against the simple "suspicious" elements alone.

That is not to say that it is unreasonable for law enforcement authorities and national security agencies to look out for the "suspicious" factors mentioned in the staff working document (the Dutch "suspicious element" of "walking fast in a suit" is too ludicrous to include, however, and simply obnoxious and illegal if the "while being black" element is added).

However, in my opinion:

For the purpose of evaluating the suitability, effectiveness and proportionality of the PNR Directive (and of the practices under the directive), a simple "hit" against these vague and far-from-conclusive factors or "criteria" should not be regarded as a "positive" result.

Rather, *a "hit" against such vague "criteria" as the purchase of an air ticket from a "suspicious" travel agent, or the using of a "suspicious" route, or the carrying of a "suspicious" amount of luggage – let alone "walking fast in a suit (while being black)" – should again only be considered a "positive result" in terms of the PNR Directive if it result in a person subsequently being formally declared to be (at least) a formal suspect in relation to terrorist or other serious, PNR-relevant criminal offences* **(see again section 5, sub-section 5.2(a), at (ab), below).**

Finally, I should note that PIU staff are not really in a position to evaluate the significance or probative value of a "hit" against these loose criteria. It must therefore be assumed that if there is such an (initial) "hit", that is always passed on to the competent authorities. In other words, the difference between initial "hits" (0.59% of all PNRs) and the confirmed "hits" that are passed on to the competent authorities (0.11%) can also not be attributable, even in part, to any manual reviews of the above matches against simple "suspicious" patterns.

(f) Matching of data in the PNRs against more complex "pre-determined criteria" or profiles

(fa) Introduction

As Article 6(3)(b) of the PNR Directive makes clear, PIUs may, in the course of carrying out their assessment under Article 6(1)(a) of whether passengers "may be involved in a terrorist offence or [other] serious crime", "process PNR data against pre-determined criteria". As also noted by the EDPS (see below), it is clear that **the PNR data can be matched against "patterns" discerned in previous data and against "profiles"**[143] **of possible terrorists and serious criminals created on the basis of these patterns, that are more complex than the simple patterns discussed at (e), above.** As I have shown at 2.2, above, this is also undoubtedly the direction in which searches for terrorists and other serious criminals are moving.

Below, I will discuss the nature of the more complex "pre-determined criteria"/"profiles"; the way they can be created, and by whom; the way they are (or are to be) applied in practice and what that means in terms of "positive" or other results; and the limitations to and the flaws in the profiles. I will discuss the consequences of the application of the criteria/profiles in sub-section 4.14, below.

(fb) The nature of the "pre-determined criteria"/"profiles"

According to footnote 36 in the staff working document:

> Pre-determined criteria, also known as targeting rules, are search criteria, based on the past and ongoing criminal investigations and intelligence, which allow to filter out passengers which corresponds to certain abstract profiles, e.g., passenger travelling on certain routes commonly used for drug trafficking, who bought their ticket in the last moment and paid in cash, etc.

[143] On the in fact rather irrelevant issue of whether the "pre-determined criteria" constitute "profiles" or not, see Box 2, overleaf.

BOX 2:

An irrelevant distraction: whether the processing discussed in this sub-section constitutes "profiling".

As the EDPS noted in his first opinion on the proposed directive:

"*One could discuss whether this type of investigation would qualify as profiling. Profiling would consist of a 'computer method making use of data mining on a data warehouse, enabling or intended to enable the classification, with some probability — and thus with some margin of error — of an individual in a specific category in order to take individual decisions towards that person'.*

The EDPS is aware that there are ongoing discussions on the definition of profiling. Whether or not it is officially recognised that the proposal aims at profiling passengers, the main point at stake is not about definitions. It is about the impact on individuals."

(paras. 20 – 21, footnote references omitted)

Definitions of "profiling" and "profile" were recently adopted by the Council of Europe:[144]

*"**Profiling**" refers to any form of automated processing of personal data, including use of machine learning systems, consisting in the use of data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.*

*"**Profile**" refers to a set of data attributed to an individual, characterising a category of individuals or intended to be applied to an individual.*

The issue appears to no longer be seriously contentious: the staff working document accompanying the Commission report on the review of the directive accepts that "profiles" are used, but appears to try and reduce the importance of this fact by repeatedly stressing that the profiles are "abstract profiles" and not "individual profiles" (see p. 18 and footnote 36) – which appears to show some ignorance about the basic methods of data mining and profiling, as discussed in the text.

All that the directive itself says in this regard is the following, in recital (7) and Article 6(4):

Recital (7):

> Assessment of PNR data allows identification of 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 by the competent authorities. By using PNR data it is possible to address the threat of terrorist offences and serious crime from a different perspective than through the processing of other categories of personal data. However, to ensure that the processing of PNR data remains limited to what is

[144] Council of Europe, Recommendation CM/Rec(2021)8 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, adopted by the Committee of Ministers on 3 November 2021 at the 1416th meeting of the Ministers' Deputies available at:
https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a46147

> necessary, **the creation and application of assessment criteria should be limited to terrorist offences and serious crime for which the use of such criteria is relevant**. Furthermore, **the assessment criteria should be defined in a manner which keeps to a minimum the number of innocent people wrongly identified by the system**.
>
> **Article 6(4):**
>
> Any assessment of passengers prior to their scheduled arrival in or departure from the Member State carried out under point (b) of paragraph 3 [i.e., in the context of "processing of PNR data against pre-determined criteria"] against pre-determined criteria shall be **carried out in a non-discriminatory manner**. **Those pre-determined criteria must be targeted, proportionate and specific.** Member States shall ensure that those criteria are set and regularly reviewed by the PIU in cooperation with the competent authorities referred to in Article 7. **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.**

As already noted, although these texts still mainly suggest the use of simple "criteria" (as discussed at (e), above), they clearly do not stand in the way of the use of much more complex ones (as long as the stipulated conditions are met).

The EDPS noted the lack of clarity in this respect already in his first opinion on the proposed directive:[145]

> **Establishing patterns and risk assessment**
>
> The proposal gives no indication on the way patterns will be established and risk assessment will be performed. The impact assessment gives the following precision as to the way PNR data will be used: *to run the data of passengers 'against a combination of characteristics and behavioural patterns, aimed at creating a risk-assessment. When a passenger fits within a certain risk-assessment, then he could be* ***identified as a high-risk passenger***'.[146]
>
> Suspected persons could be selected according to concrete elements of suspicion included in their PNR data (e.g., contact with a suspicious travel agency, reference of a stolen credit card), as well as on the basis of 'patterns' or an abstract profile. Different standard profiles could indeed be constituted on the basis of travel patterns, for 'normal passengers' or 'suspicious passengers'. These profiles would enable investigating further those passengers who do not fall within the 'normal passenger category', all the more so if their profile is associated with other suspicious elements such as a stolen credit card.
>
> Although it cannot be assumed that passengers would be targeted according to their religion or other sensitive data, it appears nevertheless that they would be subject to investigation on the basis of a mix of *in concreto* and *in abstracto* information, including standard patterns and abstract profiles.
>
> …

---

145 EDPS, (First) Opinion of the Proposal for the PNR Directive (footnote 77, above), paras. 17 – 19 and 22 – 23. The omitted paragraphs 20 – 21 deal with issue of whether the "criteria" constitute "profiles" or not, as noted in Box 2, on p. 71.

146 Impact assessment, Chapter 2.1, 'Description of the problem'. [original footnote, emphasis added]

> The main concern of the EDPS relates to the fact that decisions on individuals will be taken on the basis of patterns and criteria established using the data of passengers in general. Thus decisions on one individual might be taken, using as a reference (at least partially), patterns derived from the data of other individuals. It is thus in relation to an abstract context that decisions will be taken, which can greatly affect data subjects. It is extremely difficult for individuals to defend themselves against such decisions.
>
> In addition, the risk assessment is to be performed in absence of uniform standards of identification of suspects. The EDPS seriously questions the legal certainty of the whole filtering process, considering that the criteria against which every passenger will be scanned are so poorly defined.

As already mentioned, I will discuss the consequences of profile-based actions in sub-section 4.12, below.

Attachment 3 provides an overview of the use of "complex selectors" by the UK intelligence agencies in relation to their access to bulk communications data, prepared by Ian Brown and me in our submission on the inadequacy of UK data protection. Although many details remain hidden (in that they are redacted in the published ISC report on which the overview draws), this does show the increasing sophistication of the data mining of such bulk data sets. We conclude that the UK agencies:

> use … advanced datamining of the bulk personal datasets to identify elements and links between elements that no-one would have thought were relevant or linked in advance. Moreover, the algorithms used in the analyses are increasingly self-learning, i.e., constantly dynamically re-generated and refined through loops linking back to earlier analyses, in theory constantly improving the outcome, through "artificial intelligence". More specifically, in the search for [previously unknown] "Subjects of Interest", the software creates constantly self-improving and refining profiles against which it matches the massive amounts of data – and in the end, it produces lists of individuals that the algorithm suggests may (possibly or probably) be terrorists, or associates of terrorists.

Two points need to be made in this respect here. First of all, as noted at 2.2, above, there is no doubt that the EU and the EU Member States are increasingly seeking to produce similar profiles, based on similar data mining technologies as are used by the UK (and US) agencies, with Europol being assigned a central role in this policy.[147]

Secondly, whatever the current level of use of such sophisticated techniques in law enforcement and national security contexts in the Member States (as discussed at (fd), below), if the PNR Directive is upheld as valid in its current terms, nothing will stand in the way of the ever-greater deployment of these more sophisticated (but flawed) technologies in relation to air passengers, and that will also pave the way to yet further use of such (dangerous) data mining and profiling in relation to other large population sets (such as all users of electronic communications, or of bank cards).

147 The Fair Trial Report, Automating Injustice, I mentioned in section 2, sub-section 2.4, above (footnote 50, above) provides a series of frightening examples of the increasingly widespread use of algorithm/AI-based predictive tools in crime prevention in the Netherlands, Germany, Italy and Spain, as well as in the non-EU countries Ukraine and the United Kingdom.

(fc) The creation of the "pre-determined criteria"/"profiles"

Neither the PNR Directive, nor the proposal for the directive explain how the criteria are to be created, or indeed by whom – and the Impact Assessment only provides the most superficial of descriptions.[148] **Article 6(1)(c) says that the PIUs may "analyse PNR data for the purpose of updating or creating new criteria", but that does not preclude the original "pre-determined criteria" being created by others such as the intelligence or law enforcement agencies** – and in section 2, I have shown that in many countries including major EU Member States sophisticated work is done by those agencies precisely to the end of creating profiles for use against terrorism and other serious crime (and indeed lesser crime),[149] and that it is proposed that Europol play a central coordinating and technology-advancing role in this.

The staff working document mentions cooperation between PIUs and others:[150]

> [T]he cooperation and exchange of PNR data between the Passenger Information Units is one of the most important elements of the Directive.
>
> The regular meetings on the application of the PNR Directive, organised by the Commission, as well as the Informal Working Group on PNR, led by the Member States, have allowed for the creation of a 'EU PNR community', where national authorities can discuss, exchange ideas, share best practices and address the issues arising from the practical application of the Directive.

There is clearly cooperation with the competent authorities – which, as I have noted in sub-section 4.5, above, in "many" Member States include the intelligence services:[151]

> Most Member States have made use of the possibility to second staff from the competent authorities to the Passenger Information Units and report that this has resulted in the sharing of experiences and facilitated the development of closer relations.

And as noted in section 2, sub-section 2.2, above, Europol is also already closely involved in this, in particular through its Travel Intelligence Task Force, and this role is to be greatly expanded.

Moreover, there is nothing in the PNR Directive that says that the "pre-determined criteria" may only be created on the basis of the PNR data, i.e., that no other data can be used in that respect. If the criteria (i.e., the profiles) can be created in a collaboration between PIUs, law enforcement and intelligence agencies (as is clearly allowed and indeed encouraged), there is nothing in the PNR Directive that says this collaborative effort cannot also draw on other data than the PNR data listed in Annex I to the directive – or that profiles used by other agencies cannot be applied to PNR data (i.e., simply labelled "pre-determined criteria" for the purpose of the PNR Directive too).

---

148 See the reference in the passage from the EDPS's first opinion on the proposal for the PNR Directive, quoted later in the previous sub-section.

149 Cf. the Amsterdam Municipal Police "Top400" system, the aim of which is actually stated as not just targeting "High Impact Crime" but all forms of crime, and preventing "brothers and sisters" of "known" offenders from becoming involved with crime. Fair Trial, Automating Injustice (footnote 50, above), p. 13.

150 Staff working document (footnote 5, above), section 5.3, on p. 22.

151 *Idem*, section 3.6, on p. 8.

Given (a) the increasingly sophisticated surveillance and data analysis/data mining/risk assessment technologies developed by the intelligence services of the EU Member States (often drawing on US and UK experience) and now also by law enforcement agencies[152] and (b) the clear role assigned to Europol in this respect, it would appear clear that there is being developed a *cadre* of data mining specialists in the EU – and that the PNR data are one of the focus areas for this work.

In other words, the "pre-determined criteria" – or AI-based algorithms – that are to be used in the mining of the PNR data are being developed, not solely by or within the PIUs but by this broader *cadre* that draws in particular on intelligence experts (some of whom may be embedded in the PIUs). *The PNR databases are (also) between them a test laboratory for data mining/profiling technologies.*

And (c) there is nothing in the PNR Directive that stands in the way of using other data than PNR data in the creation of "pre-determined criteria", or indeed in the way of using profiles developed by other agencies (including intelligence agencies) as "pre-determined criteria" in the PIU analyses.

In relation to the Netherlands, the above is confirmed in the evaluation of the Dutch PNR law:[153]

> **Provision [of PNR data] on the basis of pre-determined criteria**
>
> Pi-NL [the Dutch PIU] is authorised to assess passenger data prior to the arrival in or the planned departure from the Netherlands by means of an automated comparison with risk criteria. **These criteria are created in agreement between [the PIU] and the relevant competent authorities**. A criteria set contains a specific combination of criteria with threshold values [NL: *drempelwaardes*] that are correlated with specific criminal activities and *modus operandi* relating to the offences listed in the PNR Law [i.e., PNR-relevant ofences]. …
>
> In 2020, Pi-NL carried out a match [of PNR data] against a set of pre-determined criteria that had been jointly created by [the PIU] and the unit of the *Koninklijke Marechaussee* [KMar, the Dutch national *gendarmerie*, part of the Dutch Armed Forces] that deals with human trafficking [the so-called *sluisteam*] in order to detect trafficking of minors from another EU Member State to the Netherlands (…). This matching was done twice and resulted in the provision of 273 datasets to the Kmar.[154] Right now, Pi-NL is working with competent authorities [NB: not just KMar] on the creation of six or seven new sets of pre-determined criteria.

The Dutch report does not expand on the nature of the "risk criteria" and "thresholds" – but the language – "specific combination[s] of criteria with threshold values" – clearly relates to

---

152 See again the Fair Trial report, Automating Injustice (footnote 50, above).

153 Evaluation of the Dutch PNR Law (footnote 6, above), p. 81, emphasis added. My translation. The Dutch text uses "risk criteria" [*risicocriteria*] and "set of risk criteria" [*risicocriteria-set*] for what in the PNR Directive are called "pre-determined criteria". In sub-section 4.12, below, I will note the not very promising outcomes of the 2020 exercise.

154 This number has to be qualified. 273 provisions of data does not mean 273 sets of passenger data. [original footnote, my translation] I take this to mean that separate provisions of data [*verstrekkingen*] can relate to a single person.

algorithms rather than the kinds of "simple" criteria ("single selectors") discussed at (e), above.

To the above, I may add that the fact that the staff working document notes that "*[t]he Directive does not foresee the creation of a centralised database*"[155] is not really reassuring. First of all, the sharing of data and data analyses from a range of similar but distributed databases can have the same practical effect as the establishment of a single centralised database. And the directive if anything stresses that not just PNR data and (confirmed) "hits", but also especially the "results of the processing" are to be shared between PIUs, with competent authorities, and in certain cases with Europol. In my reading, the phrase "results of the processing" clearly includes any algorithms or "risk criteria sets" developed by, and profiles created by, the PIUs (working with experts from the competent authorities and Europol). **Effectively, the *cadre* of experts, mentioned above, can share and exchange and collaborate in the creation of the "pre-determined criteria"/"profiles".**

And secondly, the reference to a centralised database not being "foreseen" in the directive as adopted if anything vaguely hints that that may change in future.[156]

(fd) The application of the more complex "pre-determined criteria"/"profiles" in practice

It would appear that to date, few Member States are as yet using data mining in relation to PNR data in as sophisticated a way as described in sub-section (fb), above (or at least acknowledge such uses):[157]

> The use of pre-determined criteria – more demanding from the operational, analytical and technical point of view – is still at an early stage of implementation in some Member States.

However, as already noted, in a range of EU Member States algorithm/AI-based profiling is already in use in relation to broader law enforcement (and especially crime prevention).[158] Moreover, the aim of the Commission and the Member States is expressly to significantly expand this use, with the help of Europol and its Travel Intelligence Task Force, and through "*training on the development of pre-determined criteria*" in "*an ongoing EU-funded project, financed under the ISF-Police Union Actions*."[159]

This merely underlines the point I made in the previous sub-sections: that the PNR database is being used as a test laboratory for advanced data mining technologies, and that if the PNR Directive is upheld as valid in its current terms, nothing will stand in the way of the ever-greater deployment of these more sophisticated (but flawed) technologies in relation to air passengers, and others. *The fact that sophisticated data mining and profiling is said to not yet be in widespread operational use in most Member States should not be a reason for ignoring this issue – on the contrary: this is the desired destination of the analyses.*

---

155 Staff working document (footnote 5, above), section 5.3, on p. 22.

156 Cf., in that respect, also the discussion in section 4.11(b), below.

157 Staff working document (footnote 5, above), section 3.5, on p. 8.

158 See yet again the Fair Trial report, Automating Injustice (footnote 50, above).

159 Staff working document (footnote 5, above), section 3.5, on p. 8. See further the discussion in section 2, sub-section 2.3, above, and the additional details in footnote 33, above.

(fe) The limitations of and flaws in the technologies

There are three main problems with algorithmic data mining-based detection of rare phenomena (such as terrorists and serious criminals in a general population) (all of which have been noted and warned about in the past, so I will draw on those earlier reports):

- The base-rate fallacy and its effect on false positives;
- Built-in biases; and
- Opacity and unchallengeability of decisions

I will discuss these in turn.

i. The base-rate fallacy and its effects on false positives

At the Court hearing in July 2021, there were some exchanges on false positive rates. These focussed on the discrepancy between the number of initial "hits" and the number of cases passed on for "further examination" by "competent authorities" that resulted in a "match". As the judge-rapporteur noted (and as also noted earlier in this opinion), according to the staff working paper there were initial "hits" in 0.59% of all one billion records checked, but only 0.11% of cases were passed on – and this was taken, by the judge-rapporteur and the other interlocuters, as suggesting a "false positive" rate of 81% (4,800,000/5,900,000) and a "true positive" rate of 19% (1,100,000/5,900,000). The judge-rapporteur wondered "whether the fallibility [*fiabilité*] of such a system [was] acceptable" and how that should be assessed:

> I would not suggest that PCR tests [to detect Covid-19 in the pandemic] are the appropriate point of reference, but given the [Covid-19 pandemic] crisis in which the find ourselves, I believe that a test with a 19% sensitivity would not be well received.

Mr von Danwitz referred to the report on PNR data prepared by me with Marie Georges in 2015 for the Consultative Committee of Convention No. 108 and to the notion of the "**base-rate fallacy**" discussed in it.[160] However, remarkably but not surprisingly, both these initial remarks and the subsequent exchanges at the hearing showed a serious lack of understanding of the statistical issues, even in relation to false-true positives and negatives, and the base-rate fallacy. This is not surprising because lawyers have long failed to properly "do" mathematics (*iudex non calculat*, as the Romans used to say). But in the digital age, mathematical and statistical ignorance is no longer acceptable. More specifically in relation to algorithm/AI-based profiling and data mining, lawyers and judges should know enough about basic mathematics and statistics to understand the issues and implications of those methodologies. Some crucial aspects of the practices are counter-intuitive – and are either not understood or deliberately obscured or even denied by proponents of such tools.

In very simple layperson's terms, the base-rate fallacy means that if you are looking for very rare instances or phenomena in a very large dataset, you will inevitably obtain a very high percentage of false positives in particular – and this cannot be remedied by adding more or somehow "better" data: by adding hay to a haystack.

[160] Douwe Korff & Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards (footnote 17, above).

In more scientific terms, the concept of the base-rate fallacy denotes the fact that "*humans in general do not take the basic rate of incidence, the base-rate, into account when intuitively solving … problems [relating to] probability*".[161] Or as Robert Matthews put it: "*[humans tend to] neglect [the importance] of prior probabilities in judging the probability of events.*"[162]

Yet taking the base rate into account is actually crucial in such contexts – and will often lead to surprising outcomes, even for those that at a rational level understand the issue. To again quote Matthews:[163]

> [D]espite its potentially serious implications for many real-life issues, the base-rate error has yet to achieve wider recognition. This is certainly true in relation to the use of algorithmic/AI-based profiling and data mining in trying to identify "known" terrorists or serious criminals (who luckily form only a minute section of the general population), and even more so in any attempt to try and predict which previously "unknown" persons might be a terrorist or serious criminal.

The mathematics are not easy to understand for non-mathematicians – let alone for lawyers: see Box 3, below.

BOX 3:

The mathematics behind the base-rate fallacy:

The base-rate fallacy is one of the cornerstones of Bayesian statistics, as it stems directly from Bayes' famous theorem (1):

$$P(A\backslash B) = \frac{P(A).P(B\backslash A)}{P(B)}$$

Expanding the probability *P(B)* for the set of all *n* possible, mutually exclusive outcomes *A* we arrive at equation (2):

$$P(B) = \sum_{i=1}^{n} P(Ai).P(B\backslash A)$$

Combining equations (1) and (2) we arrive at a generally more useful statement of Bayes' theorem:

$$P(A\backslash B) = \frac{P(A).P(B\backslash A)}{\sum_{i=1}^{n} P(Ai).P(B\backslash A)}$$

Source: Stefan Axelsson, The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection, 1999, p. 3.

---

161 Stefan Axelsson, The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection, 1999, p. 4, available at: http://www.raid-symposium.org/raid99/PAPERS/Axelsson.pdf

162 Robert Matthews. Base-rate errors and rain forecasts, Nature, Vol. 382(6594), p. 766, 29 August 1996, available at: https://www.nature.com/articles/382766a0.pdf

163 *Idem*.

However, the implications can be well described through examples. Axelsson and Matthews provide the following two examples:[164]

Example 1: (Axelsson)

Suppose that your physician performs a test that is 99% accurate, i.e. when the test was administered to a test population all of which had the disease, 99% of the tests indicated disease, and likewise, when the test population was known to be 100% free of the disease, 99% of the test results were negative. Upon visiting your physician to learn of the results he tells you he has good news and bad news. The bad news is that indeed you tested positive for the disease. The good news however, is that out of the entire population the rate of incidence is only 1=10000, i.e. only 1 in 10000 people have this ailment. What, given the above information, is the probability of you having the disease?[165]

Leaving out the formulae in which the above data are applied, that draw on those in the box, above, the result is surprising and counter-intuitive:

Even though the test is 99% certain, your chance of actually having the disease (when tested positive) is only 1/100 (i.e., 1%), due to the fact that the population of healthy people is much larger than the population with the disease. In other words, the fact that the test is positive does not say much, in absolute terms, about our state of health.

Example 2: (Matthews)

The effect of the base-rate error can be explained with reference to a familiar (indeed, notorious) dilemma - that of how to respond to weather forecasts.

It seems obvious that decisions affected by the weather (going for a walk, for example) are best made by putting one's faith in the most accurate forecast available. Surprisingly, however, the base-rate effect can make this a sub-optimal approach.

The UK Meteorological Office's 24-hour forecasts of rain currently achieve around 83 per cent accuracy, while the probability of rain on the hourly timescale relevant to walks is around 0.08. The table below reveals the impact of the base-rate error in the interpretation of forecasts of rain.

---

[164] **Example 1** is taken from Axelsson, The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection, (footnote 161, above), p. 3. The results are illustrated in a Venn diagram in Appendix A to Axelsson's paper, on p. 10. On the issue on which the paper focussed, intrusion detection, Axelsson concludes as follows:

"*[I]ntrusion detection in a realistic setting is perhaps harder than previously thought. This is due to the base-rate fallacy problem, and because of it, the factor limiting the performance of an intrusion detection system is not the ability to correctly identify behaviour as intrusive, but rather* ***its ability to suppress false alarms****. A very high standard, less than 1/100,000 per "event" given the stated set of circumstances, will have to be reached for the intrusion detection system to live up to these expectations, from an* ***effectiveness*** *standpoint. Much work still remains before it can be demonstrated that current IDS approaches will be able to live up to real world expectations of effectiveness.*" (p. 8, original emphases were in italics.)

Example 2 is taken from Robert Matthews, Base-rate errors and rain forecasts (footnote 162, above).

[165] The reader is encouraged to make a quick "guesstimate" of the answer, at this point. [original footnote]

Table:

THE VARIOUS OUTCOMES OF FORECAST AND WEATHER OVER 1,000 1-HOUR WALKS			
	Rain	No rain	Sum
Forecast of rain	66	156	222
Forecast of no rain	14	764	778
Sum	80	920	1000

With forecast accuracies of 83 per cent, one might expect that a forecast of rain during the one-hour walk would be correct 83 per cent of the time. However, the hourly base-rate of rain in the United Kingdom is so low that forecasts of rain are more than twice as likely to be wrong as right: from the table, the probability of rain, given a forecast of rain - that is, *P*(rain/forecast of rain) – is 66/222=0.30, whereas *P*(no rain/forecast)= 156/222 =0.70.

This result suggests that those who ignore Meteorological Office forecasts may fare better than those who abide by them.

Thus, unless one is particularly concerned about getting wet, the base-rate effect makes disregard of forecasts of rain the optimal strategy.

Similar reasoning also reveals that, contrary to popular belief, always carrying an umbrella is a sub-optimal strategy unless one is morbidly afraid of getting wet. Indeed, [in the vast majority of cases] the base-rate effect makes even insouciant optimism a better strategy.

These examples clearly show the counter-intuitive nature of the base-rate fallacy.

The base-rate fallacy and the use of PNR Data: (EDRi/Epicenter)

In a write-up for *European Digital Rights* (EDRi), the Austrian digital rights organisation *Epicenter* linked the issue of the base-rate fallacy to the specific matter of the use of PNR data to "identify" terrorists and other serious criminals, with a very useful illustration, as follows:[166]

The Austrian implementation of the PNR Directive

In Austria, the Austrian Passenger Information Unit (PIU) has processed PNR since March 2019. On 9 July 2019, the Passenger Data central office (*Fluggastdatenzentralstelle*) issued a response to inquiries into PNR implementation in Austria. According to the document, from February 2019 to 14 May, 7,633,867 records had been transmitted to the PIU. On average, about 490 hits per day are reported, with an average of about 3,430 hits per week requiring further verification. According to the document, out of the 7,633,867 reported records, there were 51 confirmed matches and in 30 cases there was the intervention by staff at the airport concerned.

Impact on innocents

What this small show of success does not capture, however, is the damage inflicted on the thousands of innocent passengers who are wrongly flagged by the system and who can be subjected to damaging police investigations or denied entry into destination countries

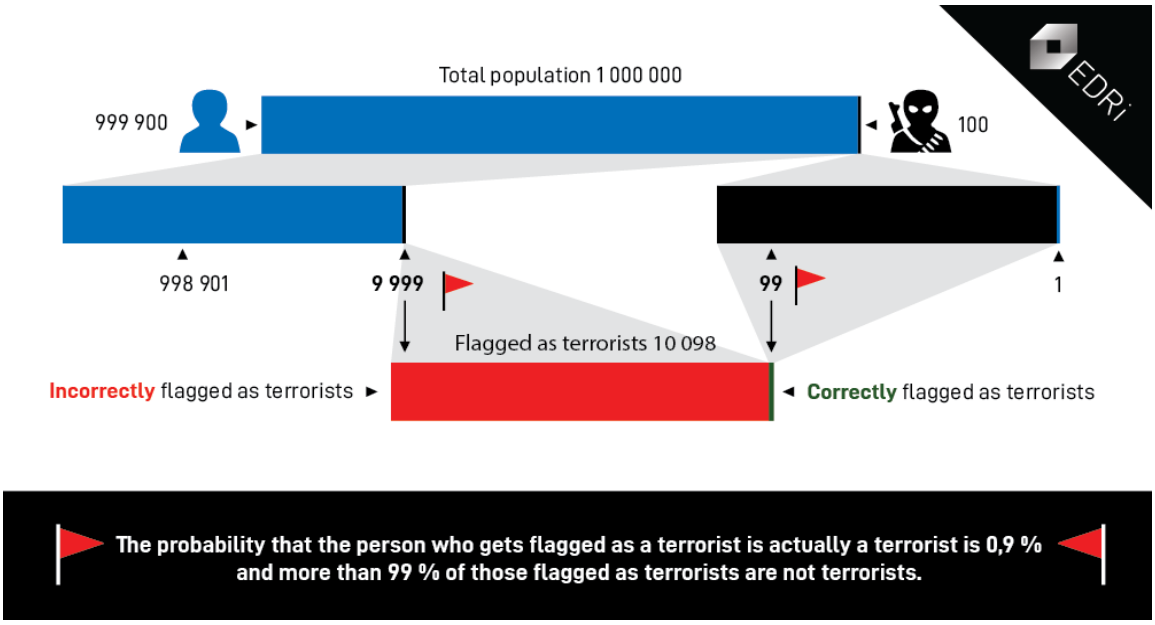
[166] Epicenter, *Why EU passenger surveillance fails its purpose*, 25 September 2019, available at: https://edri.org/our-work/why-eu-passenger-surveillance-fails-its-purpose/ (reproduced here with minor edits)

without proper cause. Mass surveillance that seeks a small, select population is invasive, inefficient, and counter to fundamental rights. It subjects the majority of people to extreme security measures that are not only ineffective at catching terrorists and criminals, but that undermine privacy rights and can cause immense personal damage.

Why is this happening? The base-rate fallacy

Imagine a city with a population of 1,000,000 people implements surveillance measures to catch terrorists. This particular surveillance system has a failure rate of 1%, meaning that (1) [in relation to persons who are actually terrorists], the system will register [this] as a "hit" 99% of the time, and fail to do so 1% of the time and (2) [in relation to persons who are not terrorists], the system will not flag them 99% of the time, but register the person as a "hit" 1% of the time. What is the probability that a person flagged by this system is actually a terrorist?[167]

At first, it might look like there is a 99% chance of that person being a terrorist. Given the system's failure rate of 1%, this prediction seems to make sense. However, this is an example of incorrect intuitive reasoning because it fails to take into account the error rate of hit detection. This is based on the base-rate fallacy: The base rate fallacy is the tendency to ignore base rates – actual probabilities – in the presence of specific, individuating information. Rather than integrating general information and statistics with information about an individual case, the mind tends to ignore the former and focus on the latter. One type of base rate fallacy is the one suggested above called the false positive paradox, in which false positive tests are more probable than true positive tests. This result occurs when the population overall has a low incidence of a given condition and the true incidence rate of the condition is lower than the false positive rate. Deconstructing the false positive paradox shows that the true chance of this person being a terrorist is closer to 1% than to 99%:



[167] As in the Axelsson example, the reader should be encouraged to make a quick "guesstimate" of the answer, at this point (cf. footnote 165, above).

Note: The matter is in fact somewhat more complicated, in that there can be different accuracy rates for true positive rates (also known, in particular in medical research, as **sensitivity**) than for true negative rates (also known in such research as **specificity**).[168] Both can only be determined by reference with reference to a so-called "**Gold Standard**" – that is, the initially hypothetically assumed level of occurrence of the issue that is being looked for (which can then be refined on the basis of subsequently obtained real data). This where the base-rate fallacy (as well as another fallacy called "anchoring") come into play. As explained in relation to medical research (with a reference to Covid-19):[169]

> Interpretation of a test result depends not only on the characteristics of the test itself but also on the pre-test probability of disease. Clinicians use a heuristic (a learned mental short cut) called anchoring and adjusting to settle on a pre-test probability (called the anchor). They then adjust this probability based on additional information. This heuristic is a useful short cut but comes with the potential for bias. **When people fail to estimate the pre-test probability and only respond to a piece of new information, they commit a fallacy called base-rate neglect [or fallacy – DK]. Another fallacy called anchoring is failing adequately to adjust one's probability estimate, given the strength of new information.** Likelihood ratios can give a clinician an idea of how much to adjust their probability estimates. Clinicians intuitively use anchoring and adjusting thoughtfully to estimate pre- and post-test probabilities unconsciously in everyday clinical practice. However, faced with a new and unfamiliar disease such as covid-19, mental short cuts can be uncertain and unreliable and public narrative about the definitive nature of testing can skew perceptions.

Astonishingly, neither the report of the Commission on the review of the PNR Directive nor the accompanying staff working document mentions the base-rate fallacy. In fact, the reports do not even mention the base rate itself: the total number of individuals on whom PNR data are collected. As explained above, the effectiveness of the processing (filtering) of those data simply cannot be measured without taking that base rate into account. Worse***: failing to take that base rate into account is precisely what leads to the base-rate fallacy.***

So what is the base rate for the PNR checks? According to Eurostat, in 2019, 1,034 million people in the EU travelled by air; in 2018 the number was just under 1,000 million.[170] However, that number reflects the total number of flights undertaken by a person – so people who fly more than once in a year are recorded as two "person-flights"; one return flight also generates two PNRs. In fact, quite a few people will have travelled by air more than once, and many not at all. A 2014 survey suggested that 52% of the UK population had not flown at all in that year, while 15% of that population had flown three or more times. On the other hand, one PNR can cover more than one person (in case of group bookings).

---

168 The terms were introduced by American biostatistician Jacob Yerushalmy in 1947, see: Jacob Yerushalmy, *Statistical Problems in Assessing Methods of Medical Diagnosis, with Special Reference to X-Ray Techniques*, Public Health Reports (1896-1970), Vol. 62, No. 40, Tuberculosis Control Issue No. 20 (Oct. 3, 1947), pp. 1432-1449, available at: https://www.jstor.org/stable/4586294 ($)

169 *Interpreting a covid-19 test result*, British Medical Journal, 2020; 369, 12 May 2020, available at: https://www.bmj.com/content/369/bmj.m1808.long (emphasis added)
The webpage contains a useful interactive "Covid-19 test calculator" on which we will draw below.

170 See footnote 93, above.

A very rough guess based on those statistics would be that on average the 1 billion people counted by Eurostat relate to 500 million distinct individuals (each taking on average two flights per year). That roughly correlates to one return trip for each EU person a year. **In other words, the base rate for PNR data can be reasonably assumed to be in the region of 500 million.**

The Commission report and the staff working document appear to imply – and certainly do nothing to refute – that the 0.11% are all "true positives". However, that glaringly fails to take account of the base rate, and its impact on results.

To expand on the EDRi/Epicentre example, above: even if the PNR checks had a failure rate of just 0.1% (meaning that (1) in relation to persons who are actually terrorists or serious criminals, the PIUs will rightly confirm this as a proper "hit" 99.9% of the time, and fail to do so 0.1% of the time and (2) in relation to persons who are not terrorists, the PIUs will rightly not generate a confirmed "hit" 99.9% of the time, but wrongly register the person as a confirmed "hit" 0.1% of the time) the probability that a person flagged by this system is actually a terrorist would still be closer to 1% than to 99%.

In any case, even if the accuracy rate of the PNR checks were to be as high as this assumed 99.9% (which of course is unrealistic), that would still lead to some 500,000 false positives each year.

Yet the Commission documentation is silent about this.

I hope that the above shows that the base-rate fallacy is of absolutely fundamental importance to any discussion of the use of PNR data. I return to this in section 5, with reference also to the question of what should, and what should not, be regarded as a "true positive". Here, I must first note the two other main problems relating to big data mining.

ii. Built-in biases[171]

It has long been known that algorithm-based assessments can be biased, even when they are entirely rational. As Marie Georges and I explained in our 2015 report, in which we also already referenced the (then still only proposed) PNR Directive:[172]

> Apart from the base rate fallacy (which is well-known to statisticians, albeit ignored by too many others …), the wider implications of algorithm-based decision-making have

[171] For more detailed discussion, see the reports already referenced in section 2, sub-section 2.4, above:
- Amnesty International, Netherlands: We sense trouble: Automated discrimination and mass surveillance in predictive policing in the Netherlands (footnote 4949, above);
- European Network Against Racism (ENAR), Data-Driven Policing: the hardwiring of discriminatory policing practices across Europe (footnote 50, above); and
- Fair Trials, Automating Injustice: the use of artificial intelligence & automated decision-making systems in criminal justice in Europe (also footnote 50, above).

See also the recent EDRi/TU Delft report, quoted later in this section (see footnote 182, below).

[172] Douwe Korff and Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards, (footnote 17, above), pp. 26 – 27.

not been as widely researched as they should be. However, the leading research in this area, by Oscar Gandy, shows that (in David Barnard-Wills paraphrase):[173]

> predictive techniques and 'rational discrimination' – statistical techniques used to inform decision making by 'facilitating the identification, classification and comparative assessment of analytically generated groups in terms of their expected value or risk' – perpetuate and enforce social inequality.

This built-in risk - that profiles will perpetuate and reinforce societal inequality and discrimination against "out-groups", including racial, ethnic and religious minorities – is of course especially acute in relation to the screening of [airline passengers].

Crucially, this can happen even if the algorithms used are in their own terms perfectly "reasonable" and indeed rational. In practice (as Gandy has shown) the results will still reinforce the inequalities and discrimination already perfidiously embedded in our societies. **Crucially, this discrimination-by-computer does not rest on the use of overtly discriminatory criteria, such as race, ethnicity or gender (which is why the "anti-discrimination" clauses in the EU-US PNR Agreement, and indeed in the proposed EU PNR Directive, are so deficient, as discussed [later in the paper and below], under the heading "*Profiling and 'sensitive data'*")**. Rather, discrimination of members of racial, ethnic, national or religious minorities, or of women, creeps into the algorithms in much more insidious ways, generally unintentionally and even unbeknown to the programmers.[174]

But it is no less discriminatory for all that. Specifically, it is important to stress that in international human rights law, the concept of discrimination does not imply some deliberate discriminatory treatment. Rather, in the words of the Human Rights Committee established under the UN Covenant on Civil and Political Rights:[175]

> the term "discrimination" as used in the Covenant should be understood to imply **any distinction, exclusion, restriction or preference** which is based on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status, and which

---

[173] Review of Gandy's main book on the topic, Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage, 2009, in *Surveillance & Society* 8(3): 379-381, at: http://www.surveillance-and-society.org/ojs/index.php/journal/article/viewDownloadInterstitial/gandy_chance/gandy_chance
For the book itself, see: http://www.ashgate.com/isbn/9780754679615 [original footnote]

[174] See in particular Fair Trials, Automating Injustice: the use of artificial intelligence & automated decision-making systems in criminal justice in Europe (footnote 49, above), section 2.1. For a particularly egregious example of bias in a widely used US system to predict re-offending, COMPAS, see: Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks, by Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, ProPublica, 23 May 2016, available at: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

[175] UN International Covenant on Civil and Political Rights, Human Rights Committee, General Comment No. 18: Non-discrimination, 10 November 1989, para. 7, emphases added, available at: http://www.unhchr.ch/tbs/doc.nsf/%28Symbol%29/3888b0541f8501c9c12563ed004b8d0e?Opendocument
The HRCtee's definition draws directly on the definitions of discrimination against women, and discrimination on the basis of race, in the major UN Conventions against discrimination against women (CEDAW) and against people on the basis of race (CERD) (and, we might add, in the UN Declaration against discrimination on the basis of religion). [original footnote]

> has **the purpose or effect** of nullifying or impairing the recognition, enjoyment or exercise by all persons, on an equal footing, of all rights and freedoms.

As we add under that heading "*Profiling and 'sensitive data'*":[176]

> [T]he provisions in the EU-third country PNR agreements (in particular in the 2012 EU-US PNR Agreement) and in the … EU PNR Directive do not really seek to prevent discriminatory outcomes of the uses of the PNR data they claim to regulate. All they do is limit (to a rather limited degree) the overt use of such data.
>
> The problem is that, as already noted, datamining and profiling almost inevitably "perpetuate and [re-]enforce social inequality" – and that this is so, irrespective of any overt limitations on the use of "sensitive data": **you can use entirely "non-sensitive" data in such operations, yet still end up with results that in effect discriminate on grounds of race, religion or sexuality etc..**
>
> Given that stigmatisation of "suspect communities" is one of the most serious dangers of any state datamining/profiling operation, no more so than in relation to terrorism, the insufficiency of the safeguards in this respect in the PNR-related instruments is another major issue of concern.

This clearly applies to the PNR Directive. At first glance, it would appear that the directive seeks to ensure that the use of the "pre-determined criteria"/"profiles" will not result in discrimination. The relevant provisions are, in particular, Articles 6(4), 7(6) and 13(4), as elaborated on in recitals 15 and 20. They read as follows:

Article 6(4):

> **Any assessment** of passengers prior to their scheduled arrival in or departure from the Member State carried out under point (b) of paragraph 3 **against pre-determined criteria shall be carried out in a non-discriminatory manner**. Those pre-determined criteria must be targeted, proportionate and specific. Member States shall ensure that those criteria are set and regularly reviewed by the PIU in cooperation with the competent authorities referred to in Article 7. **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.**

Article 7(6):

> The 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 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.**

Article 13(4):

> **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.**

---

[176] Douwe Korff and Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards, (footnote 17, above), p. 37, original emphasis, cross-reference omitted.

Recital 15:

> **[The list of the PNR data to be obtained by a PIU] should not be based on a person's race or ethnic origin, religion or belief, political or any other opinion, trade union membership, health, sexual life or sexual orientation.** ...

Recital 20:

> [**No decision that produces an adverse legal effect on a person or significantly affects that person**] **should discriminate on any grounds such as a person's 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**. The Commission should also take those principles into account when reviewing the application of this Directive.

The staff working document discusses these provisions as follows:[177]

> **Prohibition of processing of sensitive data**
>
> **The Directive prohibits the processing of 'sensitive data'** – that is, information which could reveal a person's race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life or sexual orientation (Article 13.4). **In addition, the criteria against which PNR data can be processed, cannot be discriminatory and 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** (Article 6.4). **The principle of non-discrimination also applies to decisions made by national authorities, following the processing of PNR data** (Article 7.6).
>
> The prohibition of processing sensitive data was fully transposed by a large majority of Member States, with only two exceptions. In addition, all Member States but one require an immediate deletion of such data, if collected. However, **four Member States have failed to transpose correctly the prohibition on the use of discriminatory pre-determined criteria or criteria based on sensitive data. Five Member States did not transpose the obligation that decisions of competent authorities must respect the principle of non-discrimination.**
>
> With regard to the practical realisation of the prohibition to collect and process sensitive data, national authorities report that the IT systems of the Passenger Information Unit are designed in a way that makes the collection and processing of sensitive data technically impossible. This means that such data, even if transferred by air carriers, is filtered out and blocked or deleted by the system. In addition, **the fact that sensitive data are not collected in practice excludes the possibility of designing pre-determined criteria based on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.**
>
> (emphases added)

The latter claim is repeated later on in the staff working document:[178]

> The processing against pre-determined criteria is also limited by important safeguards. **The criteria** used must be targeted, proportionate and specific to the aim pursued and

---

177 Staff working document (footnote 5, above), section 4.7.

178 *Idem*, section 5.1, under the heading "*Additional safeguards surrounding the processing of PNR data*", on p. 18.

> are subject to regular review. They **cannot be based on sensitive data and the assessment cannot be carried out in a discriminatory manner.** This limits the risk that discriminatory profiling will be carried out by the authorities.

It does not inspire confidence in the way the PNR Directive is applied in practice that four Member States have failed to transpose correctly the prohibition on the use of discriminatory pre-determined criteria or criteria based on sensitive data, and that five Member States did not transpose the obligation that decisions of competent authorities must respect the principle of non-discrimination.

But even if one leaves that aside, the document is **wrong** when it claims that "*the fact that sensitive data are not collected in practice [by the PIUs] excludes the possibility of designing pre-determined criteria based on a person's [sensitive data]*". This is because, first, as noted above, at (fc), there is nothing in the PNR Directive that bars the use of other data than the PNR data listed in Annex I to the directive in the creation of "pre-determined criteria" (in particular, if this is done in collaboration with other agencies); and indeed, it would appear that even the use of profiles created by other agencies (and that may be based on sensitive data, or proxies of such data) is not prohibited under the directive.

Second, the above claims are also **disingenuous**, in that they merely refer to avoiding the possibility of "*designing pre-determined criteria based on a person's [sensitive data]*" and of "*bas[ing] the criteria on sensitive data*". The suggestion is that if those criteria are not "based on" sensitive issues such as race, religion, etc., the application of those criteria will not result in discrimination, and indeed that no sensitive information will ever be revealed by the system:[179]

> [T]he PNR Directive strictly prohibits the processing of sensitive data. This constitutes an important difference with regard to the pre-existing draft EU-Canada PNR agreement, as explicitly acknowledged by the Court of Justice in Opinion 1/15. **The more intimate part of private life therefore remains fully protected by the processing operations provided for in the PNR Directive. Under the Directive, the information revealed by the processing of PNR data is in fact limited to the circumstances of the passenger's travel and would be established on the basis of data provided by the passengers themselves.**

That is a fundamentally misleading suggestion: as noted above, it has been shown time and again that biases can enter into algorithms and profiles even if they are not (directly) based on sensitive data – especially if proxies for such data are (knowingly or inadvertently) used.

A typical example is the "red-lining" of districts: the labelling of individuals and households in certain areas (as defined, e.g., by postcode) as constituting a "high risk" in lending terms – which has resulted in discrimination of ethnic groups concentrated in such areas.[180] Highly sensitive matters can also be deduced from seemingly innocuous data:[181]

---

179 *Idem*.

180 See CBS, *Redlining's legacy: Maps are gone, but the problem hasn't disappeared*, 12 June 2020, available at: https://www.cbsnews.com/news/redlining-what-is-history-mike-bloomberg-comments/
As the article explains, although the practice was formally outlawed in the USA in the 1970s, "some housing advocates and lawyers say the practice continues, though in different form".

181 Montreal Ai Ethics Institute, *When Algorithms Infer Pregnancy or Other Sensitive Information About People*, 2 November 2020, available at:

> Machine learning can ascertain a lot about you — including some of your most sensitive information. For instance, it can predict your sexual orientation, whether you're pregnant, whether you'll quit your job, and whether you're likely to die soon.

In simple terms: since "*intimate part[s] of [a person's] private life*" can be deduced, or at least inferred, from seemingly innocuous information – such as data included in PNRs (in particular if matched against other data) – those "*intimate aspects*" are not "*fully protected by the processing operations provided for in the PNR Directive*".

Indeed, in a way, the claim to the contrary is absurd: the whole point of "risk analysis" based on "pre-determined criteria" is to discover unknown, indeed hidden matters about the individuals who are being profiled: inferring from the data on those people, on the basis of the application of those criteria, that they are persons who "may be" involved in terrorism or other serious crimes surely is a deduction of an "intimate aspect" of those persons (even if it is not specifically or necessarily a sensitive datum in the GDPR sense – although if the inference was that a person "might be" an Islamist terrorist, that would be a [tentatively] sensitive datum in the strict sense).

Moreover, even without specifically using or revealing sensitive information, the outcomes of algorithmic analyses and processing, and the application of "abstract", algorithm/AI-based criteria to "real" people can still lead to discrimination.

The issue was recently addressed in another EDRi report, prepared at Delft Technical University, that stressed that there is:[182]

> **[a] conceptual difference between outputs and outcomes.** The outputs of the systems are the inferences they make on new data. Yet, the systems are always used in an environment where these outputs will impact things or stakeholders belonging to this environment.

---

https://montrealethics.ai/when-algorithms-infer-pregnancy-or-other-sensitive-information-about-people/
The title is a reference to an (in)famous (although possibly apocryphal) anecdote about a father learning that his teenage daughter was pregnant due to the advertising company Target sending her coupons for baby items on the basis of inferences drawn from her shopping.

[182] EDRi, *Beyond Debiasing: Regulating AI and its inequalities*, report by Agathe Balayn and Seda Gürses, Delft University of Technology, the Netherlands, September 2021, p. 24, available at: https://edri.org/wp-content/uploads/2021/09/EDRi_Beyond-Debiasing-Report_Online.pdf
The report usefully clarifies some crucial terms:
"An **algorithm** is a process or set of rules to be followed to perform a calculation.
Machine learning algorithms are the set of calculations to perform in order to produce a machine learning *model* that will perform inferences regarding the future (e.g. predicting whether an individual is likely to recidivate).
These calculations are usually made on a set of training data: *essentially, the machine learning algorithm identifies the main patterns in available data and guides the learning of an inference behaviour that copies and amplifies these patterns.*"
A **machine learning model** refers to the output of this process of algorithm execution. Concretely, it is a set of mathematical equations with parameters learned from the data using the algorithm, and which can now be used to make inferences on new data following the patterns learned from the training data. …
When talking about the entities coming out of a machine learning model when presented with a data sample, the machine learning community often interchangeably uses the terms **prediction**, **inference**, **outcome**, and **output**." (p. 23, emphases added. Note the distinction made in the text between the last two terms.)

> Thus, an outcome in this case refers to an output of a system and how it relates positively or negatively to a stakeholder.
>
> Bias and debiasing frameworks always consider the outputs of the systems, however we believe (and we will show this in the rest of the report) that considering the outcomes is more relevant when accounting for potential discrimination caused by the systems.
>
> (emphasis and underlining added)

Article 6(4) (set out in full earlier) stipulates that **the assessment[s] of passengers prior to their scheduled arrival in or departure from the Member State** carried out under point (b) of paragraph 3 of the directive with the aim of identifying persons who require further examination by the competent authorities of the directive "***shall be carried out in a non-discriminatory manner***".

In my opinion, this falls considerably short of stipulating: (i) that the "pre-determined criteria" (the outputs of the algorithms) are not biased in some way and (ii) that measures must be taken to ensure that the outcomes of the assessments are not discriminatory. It is important to address both those issues, as the EDRi report just quoted stresses.

The issue is linked to the question of whether the processing is "high risk" and therefore requires an in-depth Data Protection Impact Assessment (or more broad human rights impact assessment), as discussed in section 3, sub-section 3.3, above. As we put it in our paper, again with reference to Oscar Gandy:

> Only by constantly evaluating the results of the decisions based on profiles can one avoid these [discriminatory] effects. It takes serious effort. As Gandy concludes:[183]
>
> > these systems must be subject to active and continuous assessment and regulation because of the ways in which they are likely to contribute to economic and social inequality. This regulatory constraint must involve limitations on the collection and use of information about individuals and groups.
>
> In Europe, this "regulatory constraint" - this protection against discrimination-by-computer - takes the form of data protection rules (although, regrettably, to date not much action has been taken on this score).

The need for serious pre-evaluation of algorithms to be used in data mining and for continuous re-evaluation throughout their use is also stressed in various paragraphs in the recent Council of Europe recommendation on profiling,[184] e.g:

> 2.5 Member States should encourage the design and implementation of procedures and systems in accordance with privacy and data protection, already at their

[183] Oscar Gandy, Engaging rational discrimination: exploring reasons for placing regulatory constraints on decision support systems, J Ethics Inf Technol, Vol 12, no. 1, pp. 29-42, 2010, at: http://academic.research.microsoft.com/Publication/41860489/engaging-rational-discrimination-exploringreasons-for-placing-regulatory-constraints-on-decision [original footnote]

[184] Footnote 144, above.

> planning stage (privacy by design) and for the whole duration of data processing, notably through the use of privacy-enhancing technologies. ,,,
>
> 2.6 Profiling must not result in discrimination against individuals, groups or communities. It must undermine neither the dignity of persons nor democracy. …
>
> 2.10 The use of automated decision-making systems based on AI technologies poses additional risks due to possible errors and biases, and the difficulty of making the justification for decisions taken and ensuring transparency, consequently impeding the full exercise of the rights of the data subjects. The design, development and implementation of automated decision-making systems based on AI require special and continuous attention with regard to the risks created, and their assessment by multidisciplinary, independent teams.
>
> 3.10 Appropriate measures should be taken by the controllers and, where applicable, the processors to correct data inaccuracy factors and limit the risks of errors and biases inherent in profiling.
>
> 3.11 The controllers and where applicable, the processors should periodically and within a reasonable time re-evaluate the quality of the data and of the statistical inferences used, as well as the impact of the use of profiling on the data subject's rights.

Here, I must already note that no serious efforts have been made by the European Commission or the EU Member States to fulfil these duties. Rather (as I will note and further discuss in section 5, sub-section 5.1, below), neither have ensured that full, appropriate basic information required for such serious *ex ante* and *ex post* evaluations is even sought or recorded.

In sum: the European Commission and the EU Member States have not ensured that in practice the processing of the PNR data, and the linking of those data to other data (databases and lists), does not have discriminatory outcomes. The mere stipulation that outputs of algorithmic/AI-based profiling should not be "solely based on" sensitive aspects of the data subjects (the airline passengers) falls far short of ensuring compliance with the prohibition of discrimination.

iii. Opaqueness and unchallengeability of algorithm-based decisions including algorithm-generated "hits" (even if "confirmed" in a manual check)

In our 2015 report, Marie Georges and I also discussed the third issue with algorithmic/AI-based profiling:[185]

> [I]n the more developed "artificial intelligence" or "expert" systems, the computers operating the relevant programmes create feedback loops that continuously improve the underlying algorithms – with almost no-one in the end being able to explain the results: the analyses are based on underlying code that cannot be properly understood by many who rely on them, or even expressed in plain language.

[185] See Douwe Korff and Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards, (footnote 17, above), pp. 28 – 33. The quotes are from pp. 28 and 30 – 31 (with minor edits including references to "no-fly" lists added: the full paper explains that that is what the "misidentifications" relate to).

> …
>
> increasingly, a state agency [may] place[ ] you on a terrorist "no-fly" or "high-risk" list, "because the computer said so": because the computer generated a "score" based on a profile, that exceeded or did not reach some predetermined basic level. If you ask for an explanation (if, that is, you actually find out that such an automated decision has been made on you), the … agency (or at least the person you are dealing with) is likely to be unable to explain the decision in any meaningful way. They might provide you with examples of some of the information used (e.g., that you used a "suspicious" route, or booked your ticket from a "suspicious" travel agent), but they will not give you the underlying algorithm - partly because the official him- or herself does not know or understand that algorithm, which is in any case constantly dynamically changing, and partly because the algorithm is a "national or commercial secret".
>
> **It is extremely difficult to provide for serious accountability in relation to, and redress against, algorithm-based decisions generally.**

In our report, we referred to the fact that in relation to certain "high-risk, rules-based" (i.e., algorithmic/AI-based) terrorists lists used by the US authorities and in particular in relation to their "no-fly" lists, the relevant supervisory agency, the US Government Accountability Office (GAO), had reported that even:[186]

> the procedures [aimed at] mitigat[ing] impacts [of these lists] on passengers who may have been misidentified to these lists [i.e., who had been wrongly labelled "high risk" and barred from boarding flights] [are] considered sensitive security information –

and those "procedures" were therefore not disclosed to the barred travellers. As we already concluded then: "*That leaves those who have been thus 'misidentified' (i.e., wrongly placed on 'no-fly' lists) without redress*". We added that:[187]

> Even at a higher accountability level, e.g., in relation to parliamentary or judicial or special oversight bodies, it will be effectively impossible to verify the risks inherent in those profiles: i.e., to assess the level of "false positives" and "false negatives", or the possibly discriminatory effect of the profiles on certain groups, without the full, in-depth cooperation of the agency generating the profiles. Yet the latter are likely to be unwilling to be so helpful, unless compelled to do so by law.
>
> Profiling thus really poses a serious threat of a Kafkaesque world in which powerful agencies (like the DHS and the NSA – or in the near future European agencies?) take decisions that significantly affect individuals, without those decision-makers being able or willing to explain the underlying reasoning for those decisions, and in which those subjects are denied any effective individual or collective remedies.
>
> **That is how serious the issue of profiling is: it poses a fundamental threat to the most basic principles of the Rule of Law and the relationship between the powerful and the people in a democratic society.**

---

186 *Idem*, p. 32, with reference to section I.ii of that report, in which the "high-risk, rule-based" lists and the GAO Report are discussed in further detail.

187 *Idem*.

The issue is well illustrated by this very recent report from the UK:[188]

> **Disabled people are being subjected to stressful checks and months of frustrating bureaucracy after being identified as potential benefit fraudsters by an algorithm the government is refusing to disclose**, according to a new legal challenge.
>
> A group in Manchester has launched the action after mounting testimony from disabled people in the area that they were being disproportionately targeted for benefit fraud investigations. Some said they were living in "fear of the brown envelope" showing their case was being investigated. Others said they had received a phone call, without explanation as to why they had been flagged.
>
> **The Department for Work and Pensions (DWP) has previously conceded that it uses "cutting-edge artificial intelligence" to track possible fraud but has so far rebuffed attempts to explain how the algorithm behind the system was compiled.** Campaigners say that once flagged, those being examined can face an invasive and humiliating investigation lasting up to a year.

This case is of particular relevance because, as in relation to PNR data, the DWP system of course "merely" seeks to "identify" people who "may be" involved in crime (in that case, in fraudulently claiming state benefits), and this is then followed by "further investigation".

Also noteworthy is the consistent refusal of those developing or using the systems to be open about them. The UK Department for Work and Pensions "rebuffed attempts to explain how the algorithm behind the system was compiled". In relation to the US re-offending algorithm, COMPAS, the company that developed the system, Northpointe, first refused to disclose any details, then provided some basic information and a set of 137 questions that were used to calculate an offender's likelihood of re-offending – which turned out to be highly dubious in terms of predictive value. Yet it still refused to disclose the way it weighed the answers and calculated the relevant scores – as always claiming that this was "proprietary [information]".[189]

In the context of the use of PNR data under the PNR Directive, the opaqueness of dynamic/self-learning algorithm/AI-based profiles has effects at several different levels:

- **PIU staff cannot challenge the computer output.** The opaqueness of reasoning underpinning the computer output makes it effectively impossible for the PIU staff to determine whether an initial "hit" against "pre-determined criteria" based on algorithm-based profiles is correct or not: all they can see is that the PNR data fed into the automated system generated a "hit"; since they do not know the underlying (ever-self-"improving") algorithm, there is no way they can check the validity or otherwise of this output.*

  * As noted at 4.9(a), above, this is one reason why the large percentage of "hits" that are not confirmed by the PIU staff cannot be significantly made up of rejections of initial fully automated "hits" against the algorithm-determined profiles.

---

188 *DWP urged to reveal algorithm that 'targets' disabled for benefit fraud*, Guardian, 21 November 2021, emphasis added, available at: https://www.theguardian.com/society/2021/nov/21/dwp-urged-to-reveal-algorithm-that-targets-disabled-for-benefit?CMP=Share_iOSApp_Other

189 See Machine bias (footnote 174, above).

- **The staff of the competent authorities are unlikely (or indeed also effectively unable) to challenge the computer output.** The opaqueness makes it difficult for the staff of any competent authority to which the (supposedly "confirmed" but not really checked: see above) "hit" is reported to validate or invalidate the "hit": they too really only know that the automated system generated a "hit", and it must be assumed that most of such staff also do not know and cannot really understand the underlying (ever-self-"improving") algorithm. In addition, there is the issue of what is known as "**confirmation bias**" that takes on a special form in relation to computer-generated outputs. The term "confirmation bias" refers to the general human tendency "to search for, interpret, favour, and recall information in a way that confirms or supports one's prior beliefs or values".[190] In relation to computer-generated suggested courses of action, humans have a tendency to trust the computer suggestion: they assume the data underpinning the computer reasoning (the algorithm) to be objective, fair and reliable – even if this will often not be the case: see above, at i and ii. Employees tasked with working with computer outputs have an additional reason to "go with" the computer output: if the computer output turns out the be wrong, they can blame the computer, but if they wrongly overrode the computer suggestion, they will be held responsible for the negative consequences.

- **Supervisory bodies cannot properly assess the systems.** External supervisory bodies such as Member States' data protection supervisory authorities will generally not be given access to the underlying data, cannot review the algorithms at the design stage or at regular intervals after deployment and in any case do not have the expertise. Internal bodies are unlikely to be critical and may involve the very people who design the system (who write the code that provides the [dynamic] algorithm).

  Article 7(1) and (2) of the Dutch PNR Law stipulates that:[191]

  > [The pre-determined criteria] must be determined and regularly tested by the PIU in cooperation with the relevant competent authorities.
  >
  > [Those] criteria must be suitable for their purpose, proportionate and specific to the crime in relation to which, according to the criteria, the possible involvement of a person can be determined.

  The report on the evaluation of the Dutch PNR Law notes that, to that end:[192]

  > a special commission [has been established] that tests the pre-determined criteria (including the weighing [of the various elements] and the threshold

---

190 Wikipedia entry on *Confirmation bias*, available at: https://en.wikipedia.org/wiki/Confirmation_bias
This refers to Raymond S. Nickerson, Confirmation Bias: A Ubiquitous Phenomenon in Many Guises, Review of General Psychology, 1998, Vol. 2, pp. 175 – 220, available at: https://pages.ucsd.edu/~mckenzie/nickersonConfirmationBias.pdf

191 Original Dutch text:
1. De criteria, bedoeld in artikel 6, eerste lid, onderdeel c, worden door de Passagiersinformatie-eenheid in overeenstemming met de betrokken bevoegde instanties vastgesteld en regelmatig getoetst.
2. De criteria zijn doelgericht, evenredig en specifiek voor het misdrijf waarbij de mogelijke betrokkenheid van een persoon overeenkomstig de criteria kan worden bepaald.

192 Report on the evaluation of the Dutch PNR Law (footnote 6, above, p. 105.

> value [for regarding a "hit" against those criteria to be a valid one]) against the requirements of Article 7(2) of the Law.

The commission consists of staff of the Dutch PIU and representatives of the relevant competent authorities and of the state prosecution office (*Openbaar Ministerie*, *OM*). It is unclear – and in my opinion doubtful – whether any of the members have special expertise in relation to the matters I have discussed: the base-rate fallacy, detecting bias in outputs *and outcomes*, or checking the evolution of self-learning algorithms. In any case, they are clearly not detached from the system, or independent or impartial.

The Data Protection Officer of the PIU is not a member of the commission, but "has access to the reports" of the commission. I doubt that those reports allow the DPO (or any expert they may consult, if that is allowed) to verify the suitability, effectiveness and proportionality of the criteria. Moreover, in any case, the report adds that:[193]

> **The rules [on the creation of the pre-determined criteria] do not require the weighing [of the elements] or the threshold value [for regarding a "hit" against those criteria to be a valid one] to meet objective scientific standards.**

This is quite an astonishing matter. It acknowledges that the algorithm/AI-based profiles are essentially unscientific. In my opinion, this fatally undermines the way the pre-determined criteria are created and "tested" in the Netherlands. Yet at the same time, the Dutch system, with this "special commission", is probably better than what is in place in most other EU Member States. This surely is a matter that should be taken into account in any assessment of the PNR system EU-wide – including the assessment that is shortly to be made by the Luxembourg Court.

The only way to guard against erroneous or societally unacceptable outcomes of dynamic (self-learning) algorithm/AI-based processing and matching of data would be to have those algorithms and their application and the outcomes of their application *continuously rigorously tested and audited by fully qualified,* independent *experts on the basis of clear, peer-reviewed scientific standards in order to limit, as far as possible: straight-forward errors, bias against certain groups (especially those defined by race, gender, religion, etc.), and excessive false positives and/or false negatives. Moreover, in a democratic society the results of those tests and audits – and the underlying algorithms – should be* open to external, independent scientific review*, not least also on behalf of any individuals affected by the programs.*

At present, there is no conceivable way in which such checks and audits could be implemented: the political will is not there; the entities involved would forcefully oppose any such "interference" in their practices; and commercial entities involved in the creation of the algorithms would claim it would infringe their proprietary (intellectual property) rights. As I will show in section 5, sub-section 5.1, below, the agencies and the Member States' governments have deliberately withheld from even collecting the data that are necessary to judge the suitability, effectiveness and proportionality of their mass surveillance activities. They will not suddenly welcome openness, transparency and scientific testing of their new tools (even if, or perhaps especially because such transparency very likely would, show that those new tools are not suitable, not effective, and not proportionate to their legitimate aim).

193 *Idem*, emphasis added.

In sum:

- **because the "base-rate" for the PNR data mining is so high (in the region of 500 million people) and the incidence of terrorists and serious criminals within this population so relatively low, algorithm/AI-based profiling is likely to result in tens and possibly hundreds of thousands of "false positives": individual air passengers who are wrongly labelled to a be person who "may be" involved in terrorism or other serious crime;**
- **the provisions in the PNR Directive that stipulate that no sensitive data may be processed, and that individual decisions and matches may not be "solely based on" sensitive aspects of the individuals concerned do not protect those individuals from discriminatory outcomes of the profiling;**
- **the algorithm/AI-based outcomes of the processing are almost impossible to challenge because those algorithms are constantly dynamically changed ("improved" through self-learning) and therefore in effect impossible to fully comprehend even by those carrying out the analyses/risk assessments; and**
- **the outputs and outcomes of the algorithm/AI-based profiling and data mining and matching are not subject to proper scientific testing or auditing, and extremely unlikely to made subject to such testing and auditing.**

4.10 Direct access to PNR data by EU Member States' intelligence agencies

The whole point of the PNR Directive and the system of PIUs it establishes is to ensure that the PNR data that airlines must pass on ("push") to those PIUs in bulk are only used for the overall purposes of the directive, the prevention, detection, investigation and prosecution of terrorist offences and serious crime (see above, at 4.3) and only through the processes envisaged in the directive, including the rules on dissemination of the data discussed in the next sub-section.

While these allow for the transmission of relevant data (PNR data and analysis data) also to the intelligence agencies of the EU Member States (to the extent that those have been designated as "competent authorities" by them and provided this is subject to clear purpose-limitation: see above, at 4.5), either of the PIUs' own motion or at the request of those agencies (see sub-section 4.11, at (a) and (b)), they do not envisage granting the intelligence agencies (or any other agencies or bodies) direct access to the PNR dataset in bulk: that would seriously undermine the restrictions mentioned above.

However, it appears that at least in the Netherlands, the national intelligence agencies are granted direct access to the bulk PNR database, without having to go through the PIU (or at least without this being properly recorded).

Thus, after explaining that under the Dutch PNR law, no (electronic) records need to be kept on access to the PNR database by the Dutch intelligence and national security agencies, the report on the evaluation of the Dutch PNR Law adds, rather coyly that:[194]

> **Insofar as [read: to what extent] the intelligence and [national] security agencies have access to passenger data, this is a state secret.** [However, in the debates on the draft PNR Law,] it was reported that "PNR data are of great importance" to the intelligence and security agencies.[195] In case the intelligence and security agencies do have access to (bulk) passenger data [read: to the PNR database], it should be pointed out that under [the Dutch law on those agencies] and [relevant] policies, no retention limitation applies. In relation to all air passengers concerned, and not just suspect persons, this [read: this direct access and absence of data retention limits] might constitute a lack of transparency and safeguards in the area of privacy and data protection.

From this, it appears clear to me that the Dutch intelligence and security agencies do have direct, unrecorded access to the bulk PNR database.

The Dutch authorities may well try to argue that such direct access to data by the Dutch intelligence agencies is outside EU law. If so, I would disagree.

As it happens, Ian Brown and I discussed precisely this issue in a recent study for the European Parliament.[196] In a section on "*The national security exemption in the EU Treaties*", we wrote as follows:[197]

> **The "hole" in the EU Treaties**
>
> The EU Treaties – the founding documents of the Union – and in particular the Treaty on European Union (TEU) clarify the competences of the Union, and the limits of those competences. In particular, Article 4(1) stipulates:
>
> > competences not conferred upon the Union in the Treaties remain with the Member States.
>
> Article 4(2) adds more specifically:
>
> > 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, maintaining law and order and safeguarding national security. **In particular, national security remains the sole responsibility of each Member State.**
>
> **In simple terms: No parts of EU law, including even the EU Charter of Fundamental Rights that guarantees, inter alia, protection of personal data, apply to the activities of the EU Member States in relation to the protection of their national security.**

194 Evaluation of the Dutch PNR Law (footnote 6, above), pp. 110 – 111, emphasis added.

195 Nota van verslag van de Wet gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven (Kamerstukken II 2018/19), 34861, nr.12. [Report on the parliamentary debates] [original footnote]

196 Ian Brown & Douwe Korff, Exchanges of Personal Data After the Schrems II Judgment, study for the European Parliament's Civil Liberties (LIBE) Committee, 2021, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf

197 *Idem*, section 2.2.2, original italics, some highlights in bold original, some added.

> Consequently, all EU data protection instruments that apply to processing of personal data by authorities of EU Member States (the GDPR, the e-Privacy Directive [2002/58/EC, ePD] and the Law Enforcement Directive [2016/680, LED]) stipulate that they "*do[ ] not apply to the processing of personal data … in the course of an activity which falls outside the scope of Union law*" – i.e., in particular, to processing of personal data by EU Member States agencies in relation to activities relating to national security.[198] …
>
> **Limiting the size of the "hole"**
>
> In line with [the general approach under European fundamental rights law], the Court of Justice has restrictively interpreted the national security exemption in the Treaties. Most recently, in its Grand Chamber judgment in *La Quadrature du Net (LQDN)*,[199] the Court confirmed its earlier case-law in which it held:
>
> > although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, **the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law.**
> >
> > (*LQDN*, para. 99, with reference to earlier judgments)
>
> The Court therefore held that **the rules on personal data processing operations by entities that are, in that processing, subject to EU data protection law** (in that case, providers of electronic communication services, who are subject to the e-Privacy Directive), ***including processing operations by such entities resulting from obligations imposed on them (under the law) by Member States' public authorities*** (in that case, for national security purposes) **can be assessed for their compatibility with the relevant EU data protection instrument and the Charter of Fundamental Rights**[200] – and the Court held that laws that require "as a preventive measure, … the general and indiscriminate retention of traffic and location data" are incompatible with the Charter. [201]

In my opinion, these considerations are directly and equally applicable to the PNR data: those data (like the e-communications data at issue in *LQDN*) are processed (i.e., provided by push method to the PIUs) by the airlines under EU Member State laws (*in casu*, in the Netherlands, under the Dutch PNR Law). The processing of the PNR data is subject to EU law, i.e., the PNR Directive, the GDPR and the LED and the Charter. And "processing" includes *inter alia* disclosing and making available of the data (GDPR, Art. 4(2); LED, Art. 3(2))

I will therefore be less circumspect than the evaluators of the Dutch PNR Law: in my opinion, if the Dutch intelligence and security agencies do indeed have direct access to the PNR database, without having to go through the Dutch PIU (the Pi-NL), or without that being

198 See GDPR, Article 2(2)(a); ePD, Article 1(3) (in slightly different terms); LED, Article 2(3)(a). The EU regulation setting out the data protection rules for the processing of personal data by the EU institutions and bodies themselves (Regulation 2018/1725) does not contain such a provision because by its very nature it does not apply to processing of personal data by intelligence agencies of the Member States. [original footnote]

199 CJEU, GC judgment in Joined Cases C-511/18, C-512/18, *La Quadrature du Net v. France*, and C-520-18, *Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL and others v. Belgium*, 6 October 2020, ECLI:EU:C:2020:791. [original footnote]

200 Para. 101 (see also para. 102).

201 Para. 228. On the more specific requirements of the Charter in these regards, see section 2.3.1.3, below.

recorded – as appears to be pretty obviously the case – that is in direct breach of the PNR Directive, of the EU data protection instruments, and of the EU Charter of Fundamental Rights.

Whether the EU data protection instruments and the PNR Directive are similarly circumvented in other EU Member States, I do not know. Let me just recall that in several Member States, the PIU is "embedded in … [the] state security agenc[ies]".[202] However, the Dutch example shows how dangerous, in a democratic society, the accruing of such bulk databases is.

I will now turn to the more regulated uses of the PNR data.

4.11 Dissemination and subsequent use of the data and purpose-limitation

The PNR Directive makes provision for various ways in which PNR data, data on (confirmed) "hits", and other data resulting from the analyses of PNR data by PIUs can be provided to other entities, within their own country, in other EU Member States, and in third countries. In this, the PNR Directive distinguishes between the provision of information on a PIU's own motion ("spontaneous provision of information"), provision of information at the request of a competent authority or Europol, and provision of information to third countries on a case-by-case basis.

Below, at (a) to (c), I briefly discuss each of these in turn (making further distinctions as required). In sub-section (d), below, I will discuss the subsequent use of the transmitted data (insofar as known) and the issue in all these regards of (non)compliance with the purpose-limitation principle underpinning the PNR Directive (the principle that PNR data and the results of processing of PNR data should only be used in relation to terrorism and other serious crime ["PNR-related offences").

(a) Spontaneous provision of PNR data and information on (confirmed) "hits"

As noted earlier, under Article 6(2)(a) of the PNR Directive PIUs must:

> [carry] out an assessment of passengers prior to their scheduled arrival in or departure from the Member State [in order] to identify persons who require further examination by the competent authorities referred to in Article 7, and, where relevant, by Europol in accordance with Article 10, in view of the fact that such persons may be involved in a terrorist offence or serious crime.

If they do identify (or "identify") a person in this sense[203] (in the case of initial "hits", after a manual review: Article 6(5) and 6(6), second sentence), then in principle **the PIU must** ("shall"), **of its own motion**:

(i) transmit the PNR data of persons [thus] identified … or the result of processing those data for further examination to the competent authorities referred to in Article 7 of the same Member State. (Article 6(6), first sentence)

And:

(j) [transmit] all relevant and necessary PNR data or the result of processing those data … to the corresponding PIUs of the other Member States. The PIUs of the receiving

202 See footnote 69, above.

203 Cf. the introduction to sub-section 4.9, above.

> Member States shall transmit, in accordance with Article 6(6) [i.e., for "further examination"], the received information to their competent authorities. (Article 9(1))

NB: There is no provision for the spontaneous transmission of PNR data (or the results of the processing of such data) to Europol: Europol can only be provided with such data on request, as noted at (b), below.

In other words, in principle, subject only to a "relevant and necessary" requirement in relation to transmissions to the other PIUs, confirmed "hits" can be very widely shared across all the EU Member States, both between the PIUs but also, via the PIUs, with any "competent authority" in any Member State (including intelligence agencies where those are designated as such: see sub-section 4.5, above).

Spontaneous provision of information is, by its nature, essentially limited to matches against lists or databases of "known" persons and matches against pre-determined criteria that "identify" previously unknown persons as "persons of interest". The most important database in that respect is SIS II, but as noted in sub-section 4.9(d), above, PNR data can also be matched against national lists and data "repositories" if national law allows this. It is also important to distinguish spontaneous provision of information to a PIU's own national competent authorities from spontaneous provision of information to PIUs of other Member States (and through them to competent authorities in those other Member States).

(aa) Spontaneous provision of information to domestic competent authorities on the basis of matches against lists and databases (including SIS II)

The Commission staff working report gives no insight into the actual scope of spontaneous dissemination of PNR data or "results of the processing" of PNR data by the PIUs on the basis of (confirmed) "hits" to competent authorities in the PIUs' own countries.

The report on the evaluation of the Dutch PNR Law suggests that, in that country, spontaneous provisions of PNR to Dutch authorities "for further examination" are still effectively limited to (confirmed) matches against the SIS II database, and indeed to matches against the alerts listed in Articles 26 and 36 of the Council Decision establishing that database (respectively, alerts for persons wanted for arrest for extradition, and alerts relating to people or vehicles requiring discreet checks).[204] The Dutch PIU does not have access to police and criminal justice databases and can therefore not match the PNR data it receives against such databases (although the *Frontoffice* that has been created there can match [confirmed] "hits" against SIS II Articles 26 and 36 alerts to such other, domestic databases and can then "enrich" those "hits" with further information from those other databases).[205]

Out of the 61 million passengers whose data were checked by the Dutch PIU in 2019 and 2020, PNR data on 5,901 passengers resulted in a (confirmed) "hit" against SIS II – and as already noted in section 2, sub-section 2.3, above, 82.4% of those were matches against

[204] See footnote 131, above. In principle, matches against pre-determined criteria can also be spontaneously provided to relevant competent authorities, but to date such criteria have only been used in two test runs organised between the Dutch *gendarmerie* (KMar) and the Dutch PIU, as noted in sub-section 4.9(fc), above.

[205] Evaluation of the Dutch PNR Law (footnote 6, above), section 2.3.2, on p. 42.

"Article 36 alerts", i.e., related to "persons of interest" who were the subject of "discreet checks" etc. It would appear that all such SIS II "hits" are spontaneously provided to competent authorities in the Netherlands.[206] **The Dutch SIS II matches equate to roughly 10 in every 100,000 passengers (2:100,000 "Article 26" matches and 8:100,000 "Article 36" matches).**

If the Dutch statistics of 10:100,000 and 82.4% are representative of the overall situation in the EU, this would mean that each year, out of the 500 million passengers on whom PNR data are collected annually, approximately 50,000 passengers are subjected to "further examination" on the basis of a SIS II match, 40,000 of whom are relate to "Article 36 alerts", i.e., to "persons of interest" who are not (yet) formally wanted in relation to any crime (let alone a PNR-relevant one).

But of course, there are also (confirmed) "hits" on other bases (including on the basis of "pre-determined criteria" and matches resulting from requests for information) – and other countries may also match against more than just Article 26 and Article 36 alerts on SIS II.

(ab) Spontaneous provision of information to other PIUs on the basis of matches against lists and databases (including SIS II)

It would appear that, until now, in practice, information – including information on matches against SIS II alerts – is only rarely spontaneously shared between PIUs.

In this respect, the Commission staff working report expressly states that:[207]

> **In contrast with the widespread use of request-based information exchanges, the possibility to transfer PNR data [between PIUs] on the Passenger Information Unit's own initiative is much less prevalent. A significant number of Member State have never spontaneously transferred data to other Member States. Others use this possibility sporadically …**

In line with this, the report on the evaluation of the Dutch PNR Law reveals that:[208]

> [The Dutch PIU] did not avail itself of the possibility of spontaneous transmission [of PNR data] to another PIU in 2019, and used [this possibility] once in 2020. The [Dutch PIU] did receive [some] spontaneous transmissions [of PNR data] from PIUs of other Member States. That happened twice in 2019 and four times in 2020. In all cases it concerned another type of offence.

However, as noted at (b), below, the PIU.net project, funded under the ISF-Police Union Actions:[209]

---

206 *Idem*, p. 68; see also tables 16 and 17 on pp. 69 and 70. The numbers for SIS II matches were 2,136 for (part of) 2019 and 2,765 for 2020.

207 Staff working document (footnote 5, above), p. 22, emphasis added.

208 Evaluation of the Dutch PNR Law (footnote 6, above), p. 64, my translation. The case is briefly described in Example 6 on p. 84. The six spontaneous requests all concerned intra-EU flights (p. 67). I do not know what is meant by the reference to "another type of offence" – this may mean a not-PNR-relevant offence. That would be worrying as it would show non-compliance with the PNR Directive by the requesting PIU.

209 Staff working document (footnote 5, above), footnote 56.

> has explored the possibility of creating an application which would allow [competent authorities] to identify the Passenger Information Unit(s) which are likely to have the relevant data before a request is sent.

It would appear that if such an "application" were to be introduced, that would also significantly assist the PIUs in identifying other PIUs for which data on identified/"identified" persons could be "relevant and necessary" – and to which they should therefore decide to send the information already spontaneously, without waiting for a specific request.

The clear aim of the Commission is to significantly increase the number of spontaneous transmissions of PNR data and of information on (confirmed) "hits" against SIS II (or against pre-determined criteria: see below) between PIUs, and via PIUs to competent authorities in other EU Member States (again including intelligence agencies in Member States where those are designated as such).

(ac) Spontaneous provision of information to domestic competent authorities and to other PIUs on the basis of matches against pre-determined criteria

The Commission staff report provides just one example of a case that can be said to have been resolved on the basis of pre-determined criteria.[210] It provides no indication of the general level of (confirmed) "hits" against such criteria in the Member States, merely explaining that:[211]

> The use of pre-determined criteria – more demanding from the operational, analytical and technical point of view – is still at an early stage of implementation in some Member States.

Those Member States in which the use of predetermined criteria is still in its infancy and, to date, rarely applied (if at all) clearly includes the Netherlands, where, in 2020, there were 127 "hits" against pre-determined criteria – but those all happened in two special trials, as noted in sub-section 4.9(fc), above.

I can only conclude that it would appear that matching of PNR data against pre-determined criteria – and consequently also the spontaneous informing of competent authorities of (confirmed) "hits" against such criteria – is still extremely rare in the EU Member States. However, as noted in section 2, sub-section 2.3, the aim is for the use of such criteria to be greatly expanded.

(ad) Spontaneous provision of "results of processing" of PNR data other than information on matches against list or databases (such as SIS II) or pre-determined criteria

Neither the Commission staff working document nor the report on the evaluation of the Dutch PNR Law mentions spontaneous transmissions of "the result of processing" of the PNR data relating to identified/"identified" persons other than when they are referring to provision of information on (confirmed) "hits".

---

210 Case 6, discussed in Attachment 2. There, it is also noted that another "Case study" example, Case 11, "is more a description of what the use of 'pre-determined criteria' entails than a case study."

211 Staff working document (footnote 5, above), section 3.5, on p. 8.

However, I believe that the term "results of processing" can encompass not only "hits" against list or databases or against pre-determined criteria, but also those pre-determined criteria (profiles) themselves: they are after all to be created on the basis of analyses of PNR data (see Article 6(2)(c) of the PNR Directive). They should therefore at least be considered in this context, although, in my opinion:

The spontaneous sharing of new or improved criteria is more likely to occur within the data mining *cadre* that is being formed (see above, at 4.9(fc)), rather than done through exchanges between PIUs. But that of course does not mean that it will not occur – on the contrary, the aim is clearly to extend the use of pre-determined criteria, and for the EU Member States to cooperate much more closely in the development and sharing of those criteria, specifically through a much-enhanced role for Europol, as discussed in section 2, sub-section 2.3, above.

(b) Provision of PNR data and analysis data to competent authorities, other PIUs or Europol on request

Under Article 6(2)(b), PIUs may also, "**on a case-by-case basis**", respond to:

> **a duly reasoned request based on sufficient grounds** from [any] 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, and to provide the competent authorities or, where appropriate, Europol with the results of such processing.

In this respect, one should distinguish between provision of data in response to requests from competent authorities in a PIU's own Member State, requests from competent authorities in other Member States, and requests from Europol.

(ba) Provision of information to domestic competent authorities at the request of such authorities

In relation to the provision of information by the PIUs to their domestic competent authorities at the latter's request, the relevant national rules apply. The Commission staff working document provides no information whatsoever on the extent to which this option is used beyond saying that:[212]

> The increasing number of case-by-case requests submitted to the Passenger Information Unit by the competent authorities shows that the latter are actively using PNR data in their investigations.

In the Netherlands, any police officer and border guard[213] can request "current passenger data that are the result of a match with a database".[214] However, a request for historical

[212] Staff working document (footnote 5, above), section 5.1, on p. 16.

[213] The evaluation report refers to any investigatory officer (*opsporingsbeambtenaar*) which I believe covers both ordinary police officers and border guards.

[214] Report on the evaluation of the Dutch PNR Law (footnote 6, above), p. 108. I believe that the "current passenger data" (*aktuele passagiersgegevens*) are the same as "future passenger data" (*toekomstige passagiersgegecens*), which is the term used on the next page (p. 109) and elsewhere, which I understand refers to passengers on flights that are on their way to a Dutch airport. This is in contrast to "historical passenger data" (*historische passagiersgegevens*), i.e., data on passengers on flights in the past, as discussed in the text.

passenger data (data on passengers on flights in the past) must be authorised by a prosecutor (*officier van justitie*, *OvJ*). As the Dutch evaluation report notes, the latter is an important safeguard against undue requests for data: the OvJ checks in particular whether proposed transmissions relate to PNR-relevant offences.[215] However, this safeguard does not apply to requests for "current data".

In relation to requests that have been pre-screened by the OvJ, the evaluation report suggests that the PIU tends to assume that the requests relate to PNR-relevant offences.[216] However, overall, in 2019-20, in relation to requests for "historical data", the PIU still did not provide data in return to 40-50% of requests.[217] The reasons for this are not explained. The extent to which the PIU did not provide data in response to other requests (such as requests for "current data" by police officers) is "unknown".[218]

The Dutch evaluation report also clarifies that a single request for information can relate to a single passenger, and/or to fellow passengers (people travelling with each other, who will typically have booked together and then have only one PNR between them), or indeed to whole passenger lists (the list of all passengers on a specific flight).[219]

The Dutch evaluation report shows that over the 17 months covered, the Dutch PIU received 3,130 requests for data from Dutch authorities, mostly from the police (2,325).[220] Of these, 1,104 had a prosecution reference number (*parketnummer*), meaning that the request related to a formally opened prosecution case and therefore, presumably, to what I have called persons "formally declared to be a suspect" (or charged with, indicted for, or already convicted of) a crime under criminal [procedure] law.[221] That suggests that **the majority of requests related to early-stage investigations and to individuals who had not (yet) been formally designated as a suspect.**

Notably, the report does not mention any requests from the Dutch intelligence services – which lends credence to the suggestion that those services have direct access to the Dutch PNR database (as discussed at 4.10, above).

The Dutch report also raises doubts as to whether the data, once received by a competent authority, are really only used in relation to PNR-relevant offences;[222] I discuss this further at (d), below.

Whether other Member States impose procedural safeguards such as prior authorisation of requests from certain senior officials, I do not know. The PNR Directive does not require them (it leaves this to the laws of the Member States) and the Commission staff working report does not mention them.

---

215 *Idem*.

216 Cf. the remark on p. 108 that, if the offence in question is not mentioned in the OvJ-approved request, "the PIU can ask for clarification". The impression is that in practice this is not or rarely done.

217 *Idem*, table 16 (percentage of requests for historical data that resulted in the provision of data = 52%) and table 17 ((percentage of requests for historical data that resulted in the provision of data = 60%).

218 *Idem*, p. 69 (Table 16).

219 *Idem*, table 2 on p. 51.

220 *Idem*, p. 67. The same numbers are also provided in table 2 on p. 51.

221 *Idem*, table 2 on p. 51.

222 *Idem*, p. 108.

(bb) Provision of information to competent authorities of other EU Member States at the request of such authorities

The provision of PNR data at the request of competent authorities of other EU Member States is one part of the PNR system that is said to operate well:[223]

> **According to national authorities, the exchange of data between the Member States based on requests functions in an effective manner.** The number of requests has grown consistently and national authorities consider the possibility to request data from another Passenger Information Unit as both very useful and practical. Member States have adopted certain practical tools that facilitate the exchange of PNR data between the Passenger Information Units. For example, a large majority of Member States use a common template to request data. This helps prevent the impact of possible divergences in the interpretation of the requirement to provide due reasons for each requests. The rate of refusals is low, with most Member States having refused to share data only sporadically or having responded positively to all requests.

However, there are also some problematic aspects to this:[224]

> In terms of challenges, national authorities have pointed out to the increasing number of requests and the impact of the divergences in national regulations and practices on the cooperation between the Passenger Information Units. Some practitioners have expressed concerns that the rapidly growing number of requests received both from their own national competent authorities and the Passenger Information Units of other Member States might create an excessive workload for their Passenger Information Units and lead to longer delays in processing data. **Of particular concern is the practice of sending broad and unspecified requests to many (or even all Passenger Information Units). Such requests, even if refused as not duly reasoned, create an additional burden for the Passenger Information Unit staff.**

A footnote (footnote 56) adds to this:

> As explained before, the PNR Directive does not foresee the creation of any shared database or other centralised component. Whereas most Member States agree that the indication of a clear link with the requested Member State should be a mandatory element of a duly reasoned request, in some instances it may be difficult to determine which Passenger Information Unit may have the relevant information (e.g., if it is not known where exactly the suspect has travelled). The PIU.net project, funded under the ISF-Police Union Actions, has explored the possibility of creating an application which would allow [competent authorities] to identify the Passenger Information Unit(s) which are likely to have the relevant data before a request is sent.

Suffice it to note that implementation of this idea would bring the various PNR databases close to a confederated system – which in practice and effect is not very different from a single "centralised database" (cf. sub-section 4.9(fc), above).

---

223 Staff working document (footnote 5, above), p. 22, emphasis added.

224 *Idem*, p. 23, emphasis added.

The main text continues:

> National authorities have also pointed out to divergences in national legislation as affecting the cooperation between the Passenger Information Units. In particular, national authorities may be more or less strict in assessing if a request is duly reasoned. Some may be stricter in requiring the proof of a link between the request and their Member States, whereas others may be more flexible. The fact that the Passenger Information Units are embedded in different authorities in the Member States (Ministry of Interior, Border Guard, state security agency), and differ in terms of their competences and tasks, may also have an impact on their cooperation. The lack of harmonisation of national criminal laws leads to additional complexity in this respect. With regard to the serious crimes listed in the PNR Directive, the terminology, classification and applicable sanctions vary across the Member States, which may result in differences in the scope of application. Another problematic element is the lack of feedback – a Passenger Information Unit will not know why a particular request has been refused.

This suggests problems, in particular in relation to compliance with the purpose-limitation principle underpinning the PNR Directive. I will again return to that at (d), below.

The report on the evaluation of the Dutch PNR Law gives some insight into the numbers of requests received from other Member States and acted upon in that country, and made from there:[225]

> Between the entry into force of [the Dutch PNR Law] on 18 June 2019 and 31 December 2020, the [Dutch PIU] received 309 requests for information from PIUs in other PIUs and 66 requests for information from competent authorities of another EU Member State. [The Dutch PIU] made no requests for information to PIUs of other Member States. Since August 2020, Dutch competent authorities have submitted 73 requests for information to the [Dutch PIU] [for passing on to] a PIU of another Member State.

If the Dutch data are anything to go by, it would appear from the above that the vast majority of requests for PNR data come from the national authorities of the PIU's own country: in the Netherlands, in 2019-20, there were 3,130 requests from national authorities (see above, at (ba)), against just 375 requests from other PIUs and authorities in other EU Member States.

This rather qualifies the Commission claim that "the exchange of data between the Member States based on requests functions in an effective manner" and that "[t]he number of requests has grown consistently". Both statements could be true, but the actual total numbers of such requests may still be extremely low (for now), at least in comparison with the number of requests the PIUs receive from their own national authorities.

[225] Evaluation of the Dutch PNR Law (footnote 6, above), p. 67; see also table 6 on p. 57. Before August 2020, requests from Dutch competent authorities to PIUs of other Member States were sent directly to the latter via the Dutch national Mutual Legal Assistance Centre (*Landelijke Internationaal Rechtshulpcentrum*, *LIRC*).

(bc) Provision of information to Europol at the latter's request

Under Article 10 of the PNR Directive, Europol can also request PNR data and "results of processing" of PNR data:

> *Article 10*
>
> **Conditions for access to PNR data by Europol**
>
> 1. Europol shall be entitled to request PNR data or the result of processing those data from the PIUs of Member States within the limits of its competences and for the performance of its tasks.
>
> 2. Europol may submit, **on a case-by-case basis**, an electronic and **duly reasoned request** to the PIU of any Member State through the Europol National Unit for the transmission of specific PNR data or the result of processing those data. Europol may submit such a request **when this is strictly necessary to support and strengthen action by Member States to prevent, detect or investigate a specific terrorist offence or serious crime in so far as such an offence or crime is within Europol's competence pursuant to Decision 2009/371/JHA**. That request shall set out **reasonable grounds** on the basis of which Europol considers that the transmission of PNR data or the result of processing PNR data will substantially contribute to the prevention, detection or investigation of the criminal offence concerned.
>
> …
>
> (emphases added)

The Commission staff working document does not provide any information on the number of requests made by Europol, or on the responses to such requests from the PIUs.

The report on the evaluation of the Dutch PNR notes that within Europol there appear to be no procedural conditions or safeguards relating to the making of such requests (such as the safeguard that requests from Dutch authorities must be checked by a Dutch prosecutor (OvJ).[226]

It adds that the data protection officer of the Dutch PIU checks whether a Europol request meets the above tests (or rather: whether the request meets the principles of subsidiarity and proportionality), even though the report says that "this is not strictly required under the [Dutch] law".[227]

In 2019, the Dutch PIU did not receive any requests for historical information from Europol. In 2020, it received 24 such requests, but only provided data in response in 6 cases (=25%).[228] Since elsewhere in the report, it says that since 1 August 2020 the PIU received 32 requests for information from Europol overall,[229] it appears that in addition to the above 24 requests for historical data, it received also 8 requests for current/future data.

---

226 *Idem*, p. 109.
227 *Idem*.
228 *Idem*, table 13 on p. 64.
229 *Idem*, p. 67; see also table 6 on p. 57.

If the Dutch data are anything to go by, it would appear that there are in fact very view requests for information from Europol: in that country, the PIU only received 32 such requests between June 2019 and the end of 2020, i.e., less than two a month.
But if Europol is to be given a much more central role in the processing of PNR data, especially in the matching of those data against more sophisticated pre-determined criteria (with Europol playing the central role in the development of those more sophisticated criteria: see section 2, sub-section 2.3, above), the cooperation between the Member States' PIUs and Europol, and the sharing of PNR data and data on "hits", is certain to greatly expand.

(c) Transfer of PNR data to third countries on a case-by-case basis.

The regime for the transfer of PNR data to third countries is described in section 4.10 of the Commission staff working document as follows:[230]

> **Stricter conditions on transfer of data to non-EU countries**
>
> The transfer of PNR data by the Member States to countries outside the EU is only allowed on a case-by-case basis and **when necessary for fighting terrorism and serious crime** (that is, exclusively for the purposes for which PNR can be used under the Directive). Furthermore, **PNR data may be shared only with public authorities that are competent for combating these kinds of offences** (Article 11.1). Importantly, PNR data can only be transferred to non-EU countries only under conditions consistent with the PNR Directive and those laid down in the Law Enforcement Directive, and only upon ascertaining that the use the recipients intend to make of the PNR data is consistent with those conditions and safeguards (Article 11.3). The Data Protection Officer should be informed about every transfer of data to a third country (Article 11.4).
>
> All the Member States have established a regulatory framework for PNR data transfers to third countries that mirrors the strict limitations imposed by the Directive. In particular, the requirement that such transfers can only be made on a case-by-case basis has been transposed by all Member States. However, **four Member States have failed to fully transpose other conditions provided for by the Directive relating to the purposes for which the data can be transferred or the authorities competent to receive it.**
>
> Importantly, the law in all Member States requires that recipient third countries agree that **onward transfers to another third country can be made only with the express authorisation of the Member State whose Passenger Information Unit has transferred the data**, as required under Article 11.1(c). The Directive also provides that in exceptional circumstances such a transfer can take place also without prior authorisation if certain conditions are met, notably that the transfers are essential to respond to a specific an actual threat related to terrorist offences or serious crime in a Member State or a third country and prior consent cannot be obtained in good time (Article 11.2). **These conditions were not fully mirrored in the legislation of eight Member States.**
>
> National authorities have pointed to the active role of the Data Protection Officer in the processing of requests received from third countries. However, **in two Member States**,

230 Staff working document (footnote 5, above), section 4.10, p. 14, emphases added.

> the transposition of Article 11.4 of the Directive, requiring that the Data Protection Officer be informed each time the Member State transfers PNR to a third country, is not in conformity as the national transposing legislation restricts the role of the Data Protection Officer. In these Member States, **the Data Protection Officer is only informed in case [an onward] transfer is carried out without the prior consent of the Member State from which the data were obtained.**

It is seriously worrying that several Member States do not adhere to the conditions and safeguards relating to transfers of PNR data (and of "the results of processing" of PNR data – which can include the fact that there was a "hit" against lists or criteria) to third countries that may not have adequate data protection rules (or indeed other relevant rule of law-conform rules) in place. Some of the (unnamed) Member States that do not comply with the PNR Directive in this regard are likely to pass on such data in breach of the Directive (in particular, without ensuring that the data are only used in the fight against terrorism and serious crime) to close security and political allies such as the ones that make up the "Five Eyes" intelligence group: the USA, the UK, Australia, Canada and New Zealand.

This concern is especially aggravated in relation to the USA, which the Court of Justice has now held several times to not provide adequate protection to personal data transferred to it from the EU, specifically because of its excessive mass surveillance[231] (and there are similar concerns in relation to the UK, in spite of the Commission having issued an adequacy decision in respect of that country).[232]

The report on the evaluation of the Dutch PNR Law shows that between end-June 2019 and end 2020, the Dutch PIU received 28 requests for PNR data from third countries.[233] Provision of information in response to such requests is, in the Netherlands, subject to quite stringent conditions: the Dutch national Mutual Legal Assistance Centre (*Landelijke Internationaal Rechtshulpcentrum*, *LIRC*) checks to ensure that the provision of the data does not harm "essential national security interests" or ongoing criminal investigations in the Netherlands, and that the provision of the data is not disproportionate or irrelevant in relation to the purpose for which the information is requested; the DPO of the PIU checks that the request meets the purpose-limitation requirements of the PNR Law (and thus of the PNR Directive), i.e., relates to and is necessary in relation to PNR-relevant offences; and if already pseudonymised data are requested, a prosecutor has to approve the re-identification.[234]

However, neither the Commission staff working document nor the Dutch report provides any information on how it is – or indeed can be – guaranteed that data provided in response to a request from a third country are really only used by that third country in relation to PNR-relevant offences, or how this is – or indeed can be – monitored.

---

231 See Ian brown & Douwe Korff, Exchanges of personal data after the Schrems II judgment (footnote 196, above).

232 See Ian Brown & Douwe Korff, The inadequacy of UK data protection law in general and in view of UK surveillance laws, *Part Two on UK surveillance law* (footnote 52, above).

233 Evaluation of the Dutch PNR Law (footnote 6, above), table 6, on p. 57

234 *Idem*, p. 39.

For instance, if data are provided to the US Federal Bureau of Investigation (FBI) in relation to an investigation into suspected terrorist activity, those data will also become available to the US National Security Agency (NSA), which may use them in relation to much broader "foreign intelligence purposes".[235] That issue of course arises in relation to provision of information from any EU Member State to any third country that has excessive surveillance laws.

Moreover, if I am right to believe that the Dutch intelligence agencies have secret, unrecorded direct access to the PNR database (see above, at 4.10), they may also be sharing data from that database more directly with intelligence partners in other countries, including third countries, bypassing the whole PNR Directive system. Neither the Commission staff working document nor the report on the evaluation of the Dutch PNR law addresses this issue. And that issue, too, may well arise also in relation to other EU Member States.

(d) Subsequent use of the data and purpose-limitation

In principle, any information provided by the PIUs to any other entities, at home or abroad, or to Europol, is to be used by any recipient only for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, more specifically for the prevention, detection, investigation and prosecution of PNR-relevant offences. But it has become clear that this is far from assured in practice:

- because of the dilemma faced by PIUs in some EU Member States caused by the duty of any agency to pursue any offence that comes to their attention, the PIUs in some Member States pass on information also on (confirmed) "hits" relating to not-PNR-relevant offences (both spontaneously and in response to requests), and those data are then used in relation to the prevention, detection, investigation and prosecution of those not-PNR-relevant offences;[236]
- in the Netherlands (and probably other Member States), once information is provided to a domestic competent authority, those data enter the databases of that authority (e.g., the general police databases) and will be subject to the legal regime that applies to the relevant database – which means that there is no guarantee that their subsequent use is in practice limited to PNR-relevant offences;[237]
- when PNR data are provided by a PIU of one Member State to a PIU of another Member State (or to several or all of the other PIUs), they are provided subject to the

---

235 See Ian Brown & Douwe Korff, The inadequacy of UK data protection law in general and in view of UK surveillance laws, *Part Two on UK surveillance law* (footnote 52, above), section 2.2.2.i, *What is collected and how?*, in particular the discussion of what constitutes "foreign intelligence information" under 50 U.S. Code § 1801 – Definitions, section (e), on pp. 8 – 9.

236 See sub-section 4.9(a), above.

237 Cf. the Evaluation of the Dutch PNR Law (footnote 6, above), p. 108:
"*A competent authority [may] further process the [PNR data] or the results of the processing of those data only for the prevention, detection, investigation or prosecution of terrorist or serious crime. [This] purpose limitation is indeed set out in the form with which the information is provided, in accordance with Article 9 para. 2 of the PNR law. However, once [PNR data] are provided to a competent authority, they end up in the Law on Police Data [*Wet Politiegegevens*,* Wpg*] or another legal framework that applies to the competent authority. It is a matter outside the scope of the present study to find out whether and how the recipient of the [PNR data] assures the continued application of the purpose limitation stipulation in practice.*" (My translation)

purpose-limitation principle of the PNR Directive – but if those data are then provided by the recipient PIU(s) to competent authorities in their own countries, the same problems arise as noted in the previous indents;

- Member States take rather different views of what constitute PNR-relevant offences, and some make "broad and unspecified requests to many (or even all Passenger Information Units)" – suggesting that in this regard, too, the purpose-limitation principle is not always fully adhered to;[238]
- within Europol there appears to be no procedural conditions or safeguards relating to the making of requests for PNR data from PIUs (such as the safeguard that requests from Dutch authorities must be checked by a Dutch prosecutor)[239] and the Commission staff report does not indicate whether all the PIUs check whether Europol requests are strictly limited to PNR-relevant offences (or if they do, how strict and effective those checks are);[240]
- "four Member States have failed to fully transpose … [the] conditions provided for by the Directive relating to the purposes for which [PNR data] can be transferred [to third countries] or [relating to] the authorities competent to receive [such data]";[241] moreover:
- neither the Commission staff working document nor the Dutch report provides any information on how it is – or indeed can be – guaranteed that data provided in response to a request from a third country are really only used by that third country in relation to PNR-relevant offences, or how this is – or indeed can be – monitored;

and

- if I am right to believe that the Dutch intelligence agencies have secret, unrecorded direct access to the PNR database,[242] they may also be sharing data from that database more directly with intelligence partners in other countries, including third countries, bypassing the whole PNR Directive system. Neither the Commission staff working document nor the report on the evaluation of the Dutch PNR law addresses this issue. And that issue, too, may well arise also in relation to other EU Member States.

<u>In sum</u>: There are major deficiencies in the system as concerns compliance, by the EU Member States, by Europol, and by third countries that may receive PNR data on a case-by-case-basis, with the fundamental purpose-limitation principle underpinning the PNR Directive, i.e., with the rule that any PNR data (or data resulting from the processing of PNR data) may only be used – not just by the PIUs, but also by any other entities that may receive those data – for the purposes of the prevention, detection, investigation and prosecution of PNR-relevant offences. *In simple terms: in this respect, the PNR system leaks like a sieve.*

238 See the quote from the staff working document in sub-section (b), at (bb), on p. 105, above.
239 See sub-section (b), at (bc), above.
240 In the Netherlands, the DPO checks this, although "this is not strictly required under the [Dutch] law": see again sub-section (b), at (bc), above.
241 Staff working document (footnote 5, above), section 4.10, p. 14 – full quote in sub-section (c), above.
242 See sub-section 4.10, above.

4.12 The consequences of a "match"

As mentioned in sub-section 4.9(a), above, the staff working document stresses that:[243]

> only the data of a very limited number of passengers will be transferred to competent authorities for further processing … [and that] … overall, PNR systems deliver targeted results which limit the degree of interference with the rights to privacy and the protection of personal data of the vast majority of bona fide travellers.

I already noted there that the reference to "a very limited number of passengers" is simply dishonest: in practice, data on about 500,000 individuals are passed on annually for "further examination" by law enforcement and national intelligence/state security agencies. Moreover, given the base-rate fallacy (discussed in sub-section 4.9(f), at (fe)(i), above), the vast majority of these (confirmed) "hits" will relate to innocent persons – to what the Commission staff working paper calls "bona fide travellers". It is difficult to put a precise number on these given (a) that neither the Commission nor the Member States provide adequate quantifiable data (as discussed in section 5, sub-section 5.1, below) and (b) that it is not easy to define what constitutes a "true positive" and what a "false positive" in relation to the processing of PNR data (as already noted in section 4.9, above, and discussed in more detail in section 5, sub-section 5.2(a), at (ab), below).

However, it is quite clear that **confirmed "hits" and the associated PNR data on at the very least tens and possibly hundreds of thousands innocent people are passed on to law enforcement (and in many cases, intelligence agencies) of EU Member States and to Europol – and in some cases to law enforcement and intelligence agencies of third countries – for "further examination".**[244]

Moreover, many of those data – many of those individuals – will end up in miscellaneous national databases as (data on) "persons of interest", and/or in the Europol SIS II database as "Article 36 alerts". They may even end up in similar databases or lists of third countries.

Moreover, contrary to what the Commission and several Member States suggested at the July 2021 hearing, the effect on an innocent person of being flagged up as a (confirmed) "hit" is not trivial. For a start, at a basic legal level, the EU Charter of Fundamental Rights makes clear that the very fact that a person's personal data are being processed in itself constitutes an interference with that person's fundamental rights. This is all the more true if the processing is carried out by a law enforcement or (especially) an intelligence agency and/or the

---

243 Staff working document (footnote 5, above), section 5.1, on p. 18

244 To recall the EDRi/Epicentre example in sub-section 4.9(fe(i), even if the PNR checks had a failure rate of just 1% (meaning that (1) in relation to persons who are actually terrorists or serious criminals, the PIUs will rightly confirm this as a proper "hit" 99% of the time, and fail to do so 1% of the time and (2) in relation to persons who are not terrorists, the PIUs will rightly not generate a confirmed "hit" 99% of the time, but wrongly register the person as a confirmed "hit" 1% of the time) the probability that a person flagged by this system is actually a terrorist would still be closer to 1% than to 99%. And even if the accuracy rate of the PNR checks were to be as high as this assumed 99% (which of course is unrealistic), that would still, in relation to 500 million passengers, lead to some 50,000 false positives each year. To which I may add here that if the accuracy rate were to be 90%, that would lead to 500,000 false positives. Hence my ballpark figures above of at least tens of thousands and possibly several hundred thousands.

information is kept in a secret file (i.e., a file that is neither accessible to the public nor, as far as access to their own data is concerned, to the data subjects – meaning they are not in a position to refute the information).[245]

But of course, the PNR system is not just aimed at putting information in the files and databases of competent (law enforcement and intelligence) agencies of the EU Member States, or of Europol, or in some cases in the files and databases of third countries. Those files and databases are there to be used – used, that is, in relation to the individuals whose data are in those files and databases.

When PNR data are used in relation to individuals who are formally wanted under the laws of EU Member States (and on whom there may indeed be an "Article 26 alert" in SIS), that use takes place within a formal – and it may be assumed, in the EU Member States, rule of law-compliant – legal framework: if they are formally designated a suspect under criminal (procedure) law, they may be arrested, detained and questioned, within the limits and subject to the conditions set out in that (rule of law-compliant) framework. If they were already charged or indicted, they may be tried and (if the law allows this) detained pending trial. If they were already convicted but "on the run", they may be apprehended and taken to prison. Their privacy- and data protection rights may have been interfered with, but provided this was done within such a framework, that interference will be lawful, necessary, proportionate and entirely justified.

But the PNR data on individuals who are not formally wanted are of course also used, and used in relation to those (as yet to be presumed innocent) individuals (the majority of whom will moreover actually *be* completely innocent individuals). This comprises "known" individuals/"persons of interest" on whom there already was an "Article 36 alert" in SIS (or a similar alert in a national list or database), identified by a PIU, as well as individuals "identified" as persons who "may be" involved in terrorism or serious crime on the basis of a match against either simple criteria or against more complex profiles – who may because of this have an "Article 36 alert" entered into SIS II against them (or into a similar national watch list) when previously there had been no such alert.

At the very least, individuals put in this category will be closely watched by law enforcement and border guard officials – and possibly by intelligence agencies: being the subject of an "Article 36 alert" (or similar national alert) means being placed on a **watch list**. Those subjects, those "persons of interest", may be subjected to a "discreet check", an "inquiry check" or a "specific check" (be that under SIS II or under similar national arrangements). They may be stopped when trying to board a plane and possibly prevented from boarding – and possibly detained and questioned.

In terms of European human rights and data protection law, even the supposedly not-very-intrusive measures such as "only" being made the object of "discreet checks" constitute serious interferences with the fundamental rights of the individuals concerned – something that the European Commission and several Member States studiously avoided

[245] Cf. the European Court of Human Rights case of *Rotaru v. Romania*, judgment of 4 May 2000, which concerned a Romanian Intelligence Service file containing personal information on the applicant.

acknowledging at the Court hearing. More intrusive measure such as being detained and questioned or barred from flying of course constitute even more serious interferences. Both kinds require significant justification in terms of suitability, effectiveness and proportionality – with the onus of proof lying squarely on those who want to impose or justify those interferences, i.e., *in casu*, the European Commission and the Member States

In section 5, sub-section 5.1, below, I will show that the Commission and the Member States in fact have singularly failed to discharge this onus of proof: they have not even tried to gather relevant evidence. And in section 5, sub-section 5.2, I will show that, to the extent that one can assess the measures in terms of human rights law, they are either not suitable and ineffective to their professed end, or manifestly disproportionate to that end.

Before going there, I should add one further, final consideration – which is that **in practice "watch lists" often become "black lists"**: *should not the authorities be aware that an application for a visa or a residence permit, or for a research grant, or a sensitive job, is made by someone who is listed on an official database as someone who "may be" involved in terrorism or serious crime?*

I do not know to what extent relevant authorities dealing with such matters (immigration officials, officials vetting applicants for research grants or sensitive jobs, etc.) are granted access to databases that contain such "flags", created as a result of, or enhanced by processing under, the PNR Directive. But **history shows that people – innocent people – will suffer if there are lists of "suspicious", "perhaps not reliable", "not one of us" people lying around, and not just in dictatorships.**

That is yet another reason why those who argue in favour of such lists – and that includes "Article 36 alerts" and other lists of "persons of interest" "identified" on the basis of flimsy or complex criteria or profiles – bear a heavy onus to prove that those lists are absolutely necessary in a democratic society, and that the strongest possible measures are in place to prevent such further slippery uses of the lists.

- o – O – o -

5. The suitability, effectiveness and proportionality of the processing

5.1 The lack of data and of proof of the effectiveness of the PNR Directive (and of mass surveillance generally)

In 2011, five years after the (since invalidated) Data Retention Directive was adopted, the European Commission carried out an evaluation of the operation and effectiveness of that directive, in which it noted that:[246]

> **Reliable quantitative and qualitative data are crucial in demonstrating the necessity and value of security measures such as data retention.** This was recognised in the 2006 action plan on measuring crime and criminal justice[247] which included an objective for developing methods for regular data collection in line with the Directive and to include the statistics in the Eurostat database (providing they meet quality standards).

However:[248]s

> **It has not been possible to meet this objective, given that most Member States only fully transposed the Directive in the last two years and used different interpretations for the source of statistics.** The Commission in its future proposal for revising the data retention framework, alongside the review of the action plan on statistics, will aim to develop feasible metrics and reporting procedures which enable transparent and meaningful monitoring of data retention and which do not place undue burdens on criminal justice systems and law enforcement authorities.

It is almost unnecessary to say – but I feel still needs saying – that (as far as I know) no such "feasible metrics and reporting procedures which enable transparent and meaningful monitoring of data retention" were developed.

An in-depth study carried out in the same year at the request of the German Ministry of Justice by the Max Planck Institute for criminal law in response to a major judgment on mandatory data retention (D: *Vorratsdatenspeicherung*) of the German Constitutional Court[249] also noted **the absence of reliable statistical data** in that country, because **no empirical studies were carried out** and **data on the actual use of the mandatorily retained data, or on their effect on clearing up cases, were not collected or recorded**:[250]

---

246 European Commission, Evaluation report on the Data Retention Directive (Directive 2006/24/EC) (COM(2011) 225 final), 18 April 2011, section 4.7, *Statistics* (p. 19), emphasis added, available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF

247 Commission Communication (2006) 437, 'Developing a comprehensive and coherent EU strategy to measure crime and criminal justice: An EU Action Plan 2006 – 2010' [original footnote]

248 European Commission, Evaluation report on the Data Retention Directive (Directive 2006/24/EC) (footnote 246, above), p. 19, emphasis added.

249 Constitutional Court judgment (BVerfG-Urteil) of 2 March 2010, 1 BvR 256/08, Rn. 1-345, available at: http://www.bverfg.de/e/rs20100302_1bvr025608.html

250 Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten (Gaps [in detection and prevention of crime] caused by the ending of mandatory data retention? An investigation of the problems in relation to prevention of threats and criminal prosecution when retained telecommunication traffic data are not available), Expert Opinion (Gutachten) of the criminological section of the Max Planck Institute for foreign and international criminal law, 2nd expanded edition, July 2011, available at (e.g.): https://grundrechte.ch/2013/MPI_VDS_Studie.pdf
My somewhat free translation.

It had become clear that:[251]

> **suitable data that could form the basis of a quantitative assessment of the effects of mandatory data retention on clear-up rates [of crimes] are up to now not captured, and are also not to be captured** … because [the capturing of such data] is regarded as too expensive.

Moreover:[252]

> The European Commission is faced with a special problem in this regard. **Until now, no data have been provided that could allow for a [proper] evaluation of [the Data Retention Directive], and no such data could be provided because a suitable system of data capture** [*eine dafür geeignete Form der Datenerfassung*] **has not even been envisaged.**

A little later, the MPI report notes that:[253]

> The European Commission's evaluation report assumes that [mandatory] retention of telecommunication data has significantly contributed to European [public] security.

But it then adds that **in fact the data used were unsuited for a proper evaluation**, in particular because they did not differentiate between different data and different uses. The MPI concluded, scathingly, that:[254]

> **The statistical data provided by the [EU] Member States in no way allow for a conclusion to be drawn as to whether, and if so, to what extent, (general) [e-communications] traffic data contributed to the clearing up of crimes in criminal investigations.**

Astonishingly, history is repeating itself in relation to PNR data.

The staff working document says that:[255]

> Member States have reported that PNR processing has already actively contributed to their successes in the prevention and fight against terrorism and other serious forms of criminality, often committed by organised criminal groups. **PNR has been found to be particularly effective** to combat drug trafficking, terrorism-related offences, human trafficking and child sexual exploitation, fraud and money laundering.

This is expanded on later in the document:[256]

> In the limited time since the transposition deadline, **PNR has proven to be effective** in achieving the objective of general interest pursued. According to the Member States, the different types of processing of PNR data available to them (real time, reactive and proactive) have already delivered **tangible results** in the fight against terrorism and crime. National authorities have also highlighted that these results could not have been achieved without the processing of PNR data, e.g., by using exclusively other tools such

---

251 *Idem*, p. 218, emphasis added.
252 *Idem*, emphasis added.
253 *Idem*, p. 228.
254 *Idem*.
255 Staff working document (footnote 5, above), section 3.5, on p. 8, emphasis added.
256 *Idem*, section 5.1 on *The necessity and proportionality of collecting and processing PNR data*, on p. 15, emphases added.

> as API. Put differently, pre-existing measures were insufficient to achieve the intended objectives.

The document claims that the effectiveness of the various means of PNR processing is demonstrated, *inter alia* because:[257]

> Without claiming to be exhaustive, **Member States have provided examples** to the Commission, some of which are quoted at the end of this section, **that illustrate how the comparison of PNR data against databases and pre-determined criteria was necessary** for the identification of potential perpetrators of acts of terrorism or persons involved in other forms of serious crime, such as drug trafficking, cybercrime, human trafficking, child sexual abuse, child abduction and participation in organised criminal groups. Notably, **some cases could not have been solved without the use of PNR data**, in particular if there had been no other indication that the suspect might be involved in terrorist or other criminal activities. **In some instances, the use of PNR data resulted in the arrest of persons previously unknown to the police services, or allowed for the further examination by the competent authorities of passengers who would not have been checked otherwise.** The assessment of passengers prior to their departure or arrival has also helped prevent crimes from being committed.

In fact, the conclusion that the claim that "PNR has proven to be effective" and has "delivered tangible results in the fight against terrorism and crime" rests almost entirely on **anecdotal evidence**, not on serious analytical data. This can be deduced from a later section:[258]

> [The Commission's analysis] was informed by quantitative and qualitative information gathered by the Commission in the preparation of the review. The sources of evidence used included **Member States' statistical submissions and brief case studies** illustrating the use of PNR data, discussions in dedicated workshops and other meetings on the implementation of the PNR Directive as well as field visits to the Passenger Information Units of specific Member States. Throughout the review process, national authorities and other stakeholders involved in the practical application of the Directive were open to share information and experiences with the Commission. 57
>
> In this regard, it must be noted that **Article 20 of the PNR Directive requires Member States to collect, as a minimum, statistical information on the total number of passengers whose PNR data have been collected and exchanged, and the number of passengers identified for further examination.** As indicated above, the analysis of this information leads to the conclusion that **only the data of a very small fraction of passengers are transferred to competent authorities for further examination. Thus, the statistics available indicate that, overall, PNR systems are working in line with the objective of identifying high risk passengers without impinging on bona fide travel flows.**
>
> It should be noted that **the statistics provided to the Commission are not fully standardised and therefore not amenable to hard quantitative analysis.** This issue is compounded by the relatively early stage of development of most national PNR systems and the fact that the coverage of data collection still varies across the Member States. The Commission has mitigated these difficulties by collecting various types of evidence,

---

257 *Idem*, p. 16, emphases added.

258 *Idem*, section 5.4 on *The quality of the assessments including with regard to the statistical information gathered pursuant to Article 20*, pp. 23 – 24, emphases added.

> as discussed above, to establish a solid evidence base for the review. Importantly, in most investigations PNR data constitutes a tool, or a piece of evidence, among others, and it is thus often not possible to isolate the results attributable specifically to the use of PNR alone, or to draw conclusions on its effectiveness based solely on quantitative assessments. For this reason, a combination of quantitative and qualitative sources appears to be better suited for this type of analysis. The Commission will also continue working closely with the Member States to improve the quality of the statistical information collected under the Directive.

This strongly suggests that the only "statistical submissions" the Commission received were the minimal data mentioned: "***the total number of passengers whose PNR data have been collected and exchanged, and the number of passengers identified for further examination***".[259] **But those numbers say next to nothing about the actual effectiveness of the PNR Directive or the usefulness of the PNR data in terms of actually preventing terrorism or other forms of serious crime – and are even less informative with regard to negative consequences.**

In that latter respect, the document merely reiterates its **dishonest claim** that "*only the data of a very small fraction of passengers are transferred to competent authorities for further examination*" and adds to this the **equally misleading suggestion** that the *processing has little or no consequences for bona fide travellers*.

As noted earlier, at 4.9(a), PNR data on some 500,000 individuals are passed on for further examination each year – which may be a "small fraction" (0.11%) of the overall 500 million people covered but is certainly not trivial; and as noted at 4.12, above, being subjected to "further examination" by state authorities on the basis of a provisional assessment that one "may be" a terrorist or serious criminal is not a trivial matter either: it can have serious negative consequences, also for entirely innocent people.

The observation that such referrals do not "*imping[e] on bona fide travel flows*" is a typical disingenuous statement in this regard: perhaps *flows* of travellers are not significantly interrupted (99.89% of travellers were indeed not impeded in their travel) – but that does not mean that the lives of thousands of individual travellers who were flagged up (mostly erroneously, because of the base-rate fallacy – see section 4, sub-section 4.9(f), at (fe)(i), above – were not (possibly seriously) affected.

---

259 There may be more data in the compliance assessment of the Transposition of the EU Directive on PNR (Directive (EU) 2016/681) carried out by "Milieu Law and Policy Consulting", mentioned in footnote 3 to the staff working document. According to this footnote, "[i]t was completed on 5 September 2019 and covered the 23 Member States which notified full transposition of the Directive by 10 June 2019 (AT, BE, BG, CY, CZ, DE, EE, EL, FR, HR, HU, IE, IT, LT, LU, LV, MT, PL PT, RO, SE, SK, UK)." The assessment of the transposition measures adopted by FI and NL, which notified full transposition after 10 June 2019, and by SI, which notified only partial transposition, was still ongoing at the time the staff working document was drawn up. A Freedom of Information request was made to the Commission on 18 October 2021, asking for a copy of this compliance assessment and of the complementary assessment (if it had been completed) dealing with transposition measures adopted by FI, NL and SI. However, by the time the present opinion was finalised (1 December 2021), those documents had not (yet) been released.

Overall, typically, the "effectiveness" of the use of PNR data is measured by the Commission (if measured is the right term) in terms of (a) the extent of their use and (b) a minute number of anecdotal "case studies" that actually say nothing about the overall effects.

Specifically, the extent to which PNR data are used and the number of individuals who are referred to competent authorities for "further checking" says nothing about the effectiveness of those actions. Moreover, my analyses of these case studies in Attachment 2 show that too they reveal absolutely nothing about:

- the numbers (or percentages) of individuals who were "identified" on the basis of the various matches as warranting "further examination", but who turned out (upon such further examination, by the relevant "competent authorities") to not be terrorists or serious criminals, or indeed entirely innocent – but who are nevertheless very likely to have been significantly negatively affected by the "hit" ("**false positives**" in the broadest sense); or
- the numbers (or percentages) of actual terrorists or serious criminals who were not "identified" on the basis of the above tests as warranting "further examination", and therefore allowed to fly and not arrested on the basis of the PNR checks, i.e., of the numbers (or percentages) of **false negatives**.

As also noted in that attachment, Case 9 in particular suggests that there must be **significant numbers of false positives** – and this is in fact inevitable given the massive base rate (500 million travellers) and the relatively small numbers of actual terrorists or serious criminals within that large group (see again section 4, sub-section 4.9(f), above, in particular at (fe)(i)). I will discuss the question of what one could sensibly call "false" or "true positives" and "false" or "true negatives" further in the next sub-section.

Here, it will suffice to note that **the Commission staff working report provides no statistical evidence on which one could base a valid assessment of the effectiveness of the use of PNR data in relation to the overall aim of the PNR Directive: the prevention, detection, investigation and prosecution of terrorist offences and serious crime.**

The staff working paper suggests that "*it is … often not possible … to draw conclusions on [the PNR Directive's] effectiveness based solely on quantitative assessments*". But the real point is that **in fact no effort has even been made on the part of the Commission to even try and design suitable, scientifically valid methods and methodologies of data capture (*geeignete Formen der Datenerfassung*) that could shed light on this crucial issue.**

The same, I fear, is true in relation to **the Netherlands**. There, the researchers who evaluated the operation of the domestic PNR Law concluded that:[260]

> **The quantitative data show that the [PNR] data on intra-EU flights are in practice suitable to provide a contribution to the prevention, detection, investigation and prosecution of terrorist offences and serious crime.**

[260] Evaluation of the Dutch PNR Law (footnote 6, above), p. 7, my translation, emphasis added. The conclusion applies equally to extra-EU flights.

However, they immediately qualified that finding by adding, in the next sentence, that:

> [However,] **[t]he level of effectiveness** cannot be determined, partly because of the short time that the [Dutch] PNR Law has been in effect.

In fact, as I will note below, this impossibility also arose out of the absence of sufficient, pertinent data.

The case examples provide to the Dutch researchers by various authorities also did not help in this respect:[261]

> Because the case examples differed between them, the examples cannot be generalised and no conclusions can be drawn from them as to the effectiveness of the PNR Law.

However, because the researchers defined "effectiveness" in this context as:

> [C]ontributing [read: any contributing, no matter how minimal] to the prevention, detection, investigation and prosecution of terrorist offences and serious crime –

this provided a basis for the Minister of Justice to claim, in the letter with which he presented the evaluation report to Parliament, in my opinion **misleadingly**, that:[262]

> I conclude [note: he does not say that the researchers concluded] that **[the evaluation report] provides a positive picture of the effects and effectiveness of the PNR Law** and of the contribution that the PNR Law provides to the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

The minister also invokes the fact that the competent authorities in the Netherlands agreed that the PNR data were useful as evidence of that effectiveness.[263] Towards the end of the letter, he actually makes an even stronger claim, and attributes this to the researchers:[264]

> In conclusion, I agree with the finding of the evaluation that the PNR Law makes **an important contribution** to the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

In the next sub-section, I will take a somewhat less generous view of what can be said to be "effectiveness" in terms of the PNR Directive.

Here, I will note first that while the Dutch researchers did the best they could with the data they could find (and found considerably more data than the Commission appears to have obtained EU-wide), **those data were still manifestly insufficient for use as a basis for serious conclusions as to the effectiveness of the PNR law or of the use of the PNR data in the Netherlands**. Below, I reproduce selections from the list of missing data, set out in the evaluation report itself, paraphrased by me and interspersed with quotes from various specific references to such omissions in the text:[265] I add some further categories at the end.

---

261 Evaluation of th Dutch PNR law (footnote 6, above), p. 74, my translation.

262 Letter of the Minister for Justice and Security to the President of the First Chamber of the Dutch Parliament, 12 November 2021, p. 1, my translation, emphasis added, available at: https://www.eerstekamer.nl/behandeling/20211112/brief_van_de_minister_van_j_v_met/document3/f=/vlnzbci3ggy5.pdf

263 *Idem*, p. 2. Those (unquantified) claims are reported in some detail in section 4.3 of the evaluation report, on *Perceived usefulness of the use of PNR data*, on pp. 85 – 87.

264 *Idem*, p. 8, emphasis added.

265 Evaluation of the Dutch PNR Law (footnote 6, above). The full list is set out on pp. 50 – 51 and numbered. Because I only reproduce some of the items, I have omitted the numbers. Where I have inserted

Missing data

The following data are missing:

Re the collection of PNR data:

- The number of PNRs received. The number of air passengers on whom at least once PNR data were received by the Dutch PIU is known. However, because PNR data are in principle, but not always, sent three times (48 and 24 hours before departure and at check-in), **it is not possible to calculate the percentage of PNRs in relation to which there was am initial "hit" and/or a passing-on of a (confirmed) "hit"**.

Re the processing and provision of PNR data:

- The number of passengers on whom there was an automated match. The total number of automated matches is known,[266] but the total number of passengers in relation to whom there was a match is not known. This means that it is, for instance, not known whether one hundred matches related to the same frequent flyer or to a hundred different passengers. This means that the percentage of passengers on whom there was an automated match cannot be calculated.
- *Although the total number of automated (initial) "hits" is known, the total number of confirmed "hits" that were passed on for further examination is not (chart on p. 66).*
- *The data on confirmed "hits" that were passed on for further examination do not distinguish between confirmed "hits" related to terrorist offences and confirmed "hits" related to other serious criminal offences (p. 68).*
- The total number of passengers on whom data were provided [to competent authorities] (partially unknown). The number of passengers on whom data were provided [to competent authorities] is known. This number however excludes fellow travellers and complete flight lists. This means that a passenger whose data have been provided are not included in the total if he or she travelled with someone on whom there was match, or if he or she was included in a complete flight list together with someone in relation to whom such a complete list was requested. This means that the official tally is lower than the real numbers.
- *From the moment at which PNR data or the results of processing of PNR data leave the PIU and the Frontoffice,[267] the use of the data are not recorded in a standardised way in the databases of the relevant competent authorities. Because of this, at the moment it is impossible to obtain a complete view of the whole processing chain (p. 74).*
- *The results of the use of PNR data provided as a result of confirmed "hits"[268], i.e., the actual actions undertaken as a direct consequence of the receipt of this information (in particular by the Dutch* gendarmerie*, KMar), are at present insufficiently recorded; there are plans to improve the recording by KMar and to*

references to the relevant missing data from other places in the text, I have either *italicised* the text or placed it in boxes and provide the page reference in brackets. Emphases added.

266 The numbers were 115,000 in 2019 and 77,000 in 2020 (when there were less flights because of the Covid pandemic): evaluation report, p. 60.

267 See footnote 66, above.

268 Referred to in the Dutch report as "alerts": see again footnote 66, above.

report back on such results of the provision of PNR data to the PIU (p. 74), but the prosecuting and judicial authorities say it would be too much effort to record the results of the use of PNR data in criminal records (p. 75)

- *According to an earlier impact assessment of the Law, it was "not or hardly possible" to keep records even of the fact that PNR data are included in an investigation file, let alone the extent to which those data contribute to the resolution of the case (p. 75).*[269] *Consequently:*

> **"There are no quantitative data on the way in which [and the extent to which] PNR data have contributed to the prevention, detection, investigation and prosecution of terrorist offences and serious crime.**
>
> **There is also no information as to the number of provisions of PNR data to competent authorities in which it turned in the end that they did not concern the right person; so-called '*false positives*'.**[270]
>
> **This does not only make it impossible to determine the effectiveness of the use of PNR data. It would also appear to render supervision over compliance with the purpose-limitation principle in the PNR Law virtually impossible."** (p. 75)

- *There are to date no data on the use of PNR data in criminal proceedings and no known judgments in which a criminal court referred to them as evidence. The Judicial Council is examining whether further insight can be obtained (p. 75).*
- *In relation to the only use of pre-determined criteria (in two test runs),*[271] *25% of the matches turned out to be correct (which means there was a 75% false positive rate – DK), but it could not be determined whether (even) these 25% "correct matches" related to PNR-relevant offences (p. 81).*[272]
- *Little can be concluded with regard to the results or effects of the use of PNR data obtained as a result of requests from competent, in relation to the fight against serious criminality or terrorism. The requests do not show what role the data played in criminal investigations or how essential they were in that regard.*

The overall conclusion of the researchers is that:

> "The quantitative insights and the illustrative examples provide a partial indication of how PNR data re used in practice. Up to a point, **the demand for PNR data from competent authorities** provides an indication of their use, but it **says nothing about the results or their effects on the fight against terrorist and serious criminal crimes**. The illustrative examples clarify the role that PNR data played in specific criminal investigations, but cannot be generalised." (p. 94, emphasis added)

---

269 As already noted in footnote 127, above, this impact assessment, carried out in 2020, and known as the Ketenbrede Impact Assessment, was not a data protection impact assessment, but sought to assess the impact of the application of the law on the workload of the various authorities.

270 I believe that there are also (many) false positives other than the ones mentioned here. I discuss this in the next sub-section.

271 See section 4, sub-section 4.9(fc), above.

272 In my opinion, if they did not relate to PNR-relevant offences, they should also not be regarded as "true positives". I again discuss this further in the next sub-section.

To the above, **I would add the following categories of missing data**:

- Information on the results of the provision of PNR data to competent authorities in the PIUs' own countries, in other Member States, or to Europol:
- *There are no data on the number or percentages of (confirmed) "hits" that resulted in an "Article 36 SIS alert" being issued on the individuals concerned, or of the number of percentages of (confirmed) "hits" resulting in those individuals being designated "persons of interest" under national lists;*
- *There are no data on the number or percentages of (confirmed) "hits" that resulted in the individuals concerned being formally declared to be a suspect under criminal or criminal procedure law in relation to a PNR-relevant offence, or formally charged or indicted or convicted of such an offence – and not even any indication of the numbers or percentages of (confirmed) "hits" that significantly contributed to such outcomes;*
- *There are no data on how long "Article 32 alerts" on persons on whom such alerts had been issued on the basis of a (confirmed) "hit" stay in the SIS II database (in relation to persons who were not formally declared suspects in relation to, or charged with, indicted for or convicted of, PNR-relevant offences);*
- *There are no data – not even any estimated data – on the number or percentages of actual terrorist or serious criminals who are "missed" by the system, i.e., on whom there were no (confirmed) "hits".*

In sum: Neither the European Commission's review nor the Dutch evaluation has come up with serious, measurable data showing that the PNR Directive and the PNR law are effective in the fight against terrorism or serious crime.

The Dutch researchers at least tried to find hard data, but found that in many crucial respects (listed above) no records were kept that could provide such data. At most, some suggestions for better recording were made, and some ideas are under consideration, to obtain better data (although the researchers also noted that some law enforcement practitioners thought it would be too much effort).

To date, neither the Commission nor the Member States (including the Netherlands) have seriously tried to design suitable, scientifically valid methods and methodologies of data capture (*geeignete Formen der Datenerfassung*) in this context. Given that the onus is clearly on them to demonstrate – properly, scientifically demonstrate, in a peer-reviewable manner – that the serious interferences with privacy and data protection they insist on perpetrating are effective, this is a manifest dereliction of duty.

The excuse for not doing this essential work – that it would be too costly or demanding of law enforcement time and staff – is utterly unconvincing, given the many millions of euros that are being devoted to developing the "high risk" intrusive technologies themselves.[273]

[273] See footnote 33, above.

5.2 Assessing the suitability, effectiveness and proportionality of the processing of PNR data under the PNR Directive

(a) The appropriate tests to be applied

(aa) The general tests

As already noted at 4.2, above, if one wants to assess the suitability, effectiveness and proportionality of a measure, one must first of all define the aim of the measure. In relation to the use of PNR data under the PNR Directive, this aim is:[274]

> the prevention, detection, investigation and prosecution of terrorist offences and serious crime
>
> (Title and Article 1(2))

If a measure, if applied, constitutes a serious interference with the interests or fundamental rights of those affected, it constitutes a "high risk" measure that requires very strong justification.

In section 4, sub-section 4.12, I concluded that:

> contrary to what the Commission and several Member States suggested at the July 2021 hearing, the effect on an innocent person of being flagged up as a (confirmed) "hit" is not trivial.

And that:

> In terms of European human rights and data protection law, even the supposedly not-very-intrusive measures such as "only" being made the object of "discreet checks" constitute serious interferences with the fundamental rights of the individuals concerned – something that the European Commission and several Member States studiously avoided acknowledging at the Court hearing. More intrusive measure such as being detained and questioned or barred from flying of course constitute even more serious interferences. Both kinds require significant justification in terms of suitability, effectiveness and proportionality – with the onus of proof lying squarely on those who want to impose or justify those interferences, i.e., in casu, the European Commission and the Member States

In my opinion, the appropriate tests to be applied to mass surveillance measures such as are carried out under the PNR Directive (and were carried out under the Data Retention Directive, and are still carried out under the national data retention laws of the EU Member States that continue to apply in spite of the CJEU case-law) are:

Have the entities that apply the mass surveillance measure – i.e., in the case of the PNR Directive (and the DRD), the European Commission and the EU Member States – produced reliable, verifiable evidence:

(i) that those measures have actually, demonstrably contributed significantly to the stated purpose of the measures, i.e., in relation to the PNR Directive, to the fight

[274] For a more detailed discussion, see section 4, sub-section 4.3, above.

against PNR-relevant crimes (and in relation the DRD, to the fight against "serious crime as defined by national law"); and

(ii) that those measures have demonstrably not seriously negatively affected the interests and fundamental rights of the persons to whom they were applied?

If the mass surveillance measures do not demonstrably pass both these tests, they are fundamentally incompatible with European human rights and fundamental rights law.

This means the measures must be justified, by the entities that apply them, on the basis of hard, verifiable, peer-reviewable data.

(ab) When a (confirmed) "hit can be said to constitute a "positive" result (and when not)

In the context of collecting and assessing data, it is important to clarify when a (confirmed) "hit can be said to constitute a "positive" result (and when not).

The discussions at the Court hearing in July 2021 appeared to be based on a common view among the participants that the suitability, effectiveness and proportionality of the PNR Directive could be assessed by reference to the number of initial "hits" noted by the PIUs (0.59% of cases), compared to the number of confirmed "hits" passed on for "further examination" to the competent authorities (0.11%), i.e., that there was a "false positive" rate of approximately 80% (see section 4, sub-section 4.9(f), at (fe)(i), above). But that is **fundamentally wrong**: it ties in with the Commission and Dutch minister's (equally erroneous) belief that the effectiveness of the use of PNR data can be "proven" by the fact that they are increasingly widely used (see sub-section 5.1, above).

But as noted above, the only really appropriate assessment of the effectiveness of the PNR Directive must be the actual, measurable impact the use of the PNR data has had on preventing, detecting, investigating and prosecuting terrorist offences and serious crime.

To echo the conclusions of the Dutch researchers: **the number of (confirmed) "hits" that are passed on for "further examination" to competent authorities at home or abroad (or to Europol or third countries), *says nothing about the results or their effects on the fight against terrorist and serious criminal crimes*, and the illustrative examples provided by the Commission and the Dutch authorities "clarify the role that PNR data played in specific criminal investigations, but cannot be generalised".**[275]

Given that in the absence of proper data it is impossible to measure the actual, final results or effects of (confirmed) "hits", or the outcomes of the "further examinations", it is impossible to reach firm conclusions about the real effectiveness of the use of the PNR data. However, I believe that some pertinent observations can still be made as to when an outcome can (tentatively) be said to constitute a "true positive" and when not.

In my opinion, **it is acceptable to regard a (confirmed) "hit" – a confirmed matching of basic identity data – in relation to "known" formally wanted persons as a "positive result" for the purposes of the PNR Directive provided that the person was wanted (formally suspected of, charged with, or convicted of) PNR-relevant offences** – after all, the persons were so marked

[275] Cf. Evaluation of the Dutch PNR Law (footnote 6, above), p. 94, quoted at 5.1, above, emphasis added.

on the basis of a proper process, typically under the criminal- or criminal procedure law, by a judge or senior prosecutor (although there will of course still be cases in which the identification will still prove to have been erroneous after further checks, which should be regarded as "false positives").

But a (confirmed) "hit" in relation to persons who are wanted in relation to non-PNR-relevant offences should – of course – not be regarded as a positive result under the PNR Directive.

Moreover, I firmly believe that **it is wrong to regard all confirmed "hits" relating to "known" "persons of interest" (including all [confirmed] "hits" relating to "Article 36 SIS alerts") and all persons "identified" (labelled) by the PIUs as "persons who *may be* involved in terrorism or serious crime" as in some way a (true) positive result in terms of the aim of fighting terrorism and other serious crime.**

This is because not all "persons of interest"/subject of "Article 36 alerts" will be persons in relation to whom there are actual indications of involvement in terrorism or serious crime: a person can be listed as a "person of interest" (especially by the intelligence agencies) for all sorts of reasons; it can include witnesses and even victims, or persons with only the most indirect, tenuous links to any such crimes, or indeed any crimes, such as fellow travellers or relatives – and to mark a person as a "person of interest" can have serious, pernicious effects (as discussed in section 4, sub-section 4.12, above). In that regard, it should be recalled that (according to the Dutch figures) **more than 80% of all (confirmed) "hits" were against "Article 36 SIS alerts"**.[276] **Those should <u>not</u> automatically all be counted as "true positives".** I discuss this further in my final, overall conclusions in sub-section 5.3, below.

Furthermore, **"identifying" persons as "possibly" involved in terrorism or serious crime on the basis of vague "suspicious" elements (ticket bought from a "suspicious" travel agent; using a "suspicious" travel route; etc.) or because of matches against "pre-determined criteria" or more complex "abstract profiles" is in fact only a statement of a probability** – and because of the "base rate fallacy" (explained in sub-section 4.9(f), above, at (fe)(i)), the probability of any person so marked actually being a real terrorist or serious criminal is incredibly low (even if there will of course also be some actual terrorists and serious criminals who are correctly so labelled). The mere fact that there is such a match, such an assumed probability can in my opinion not suffice to regard the "hit" as a (true) positive. Rather:

In my opinion, confirmed "hits" confirming the identity of "known" "persons of interest"/subjects of "Article 36 alerts" and the "identification" (labelling) of previously "unknown" persons by the PIUs as "persons who *may be* involved in terrorism or serious crime" can only be regarded as "positive" results under the PNR Directive if those "hits" result in those persons subsequently being formally declared to be formal suspects in relation to terrorist or other serious, PNR-relevant criminal offences.

[276] See sections 2.3 and 4.7, above, and the reference in footnote 28, above.

(b) The failure of the European Commission (and the Dutch government) to meet the appropriate tests

The conclusion reached by the European Commission and Dutch Minister of Justice and noted in the previous sub-section: that overall, the PNR Directive, respectively the Dutch PNR law, had been "effective" because the EU Member States said so (Commission) or because PNR data were quite widely used and the competent authorities said so (Dutch Minister) is fundamentally flawed, given that this conclusion was reached in the absence of any real supporting data.

It is the equivalent to a snake oil salesman claiming that the effectiveness of his snake oil is proven by the fact that his franchise holders agree with him that the product is effective, or by the fact that many gullible people bought the stuff.

Or to use the example of Covid vaccines, invoked by the judge-rapporteur: it is equivalent to a claim that a vaccine is effective because interested parties say it is, or because many people had been vaccinated with the vaccine – without any data on how many people were protected from infection or, perhaps worse, how many people suffered serious side-effects.

Of course, in relation to vaccines, there are regulators who would not allow a vaccine on the market until it had been shown in scientifically sound trials producing solid, peer-reviewed data, to have been effective in preventing disease, without causing serious side-effects.

In the case of mass surveillance measures – be that mandatory e-communications data retention or the mass collection and analysis of PNR data – the regulator (the entity that is supposed to ensure that measures are effective and do not cause undue harm) is the European Commission, assisted by the Member States. But disgracefully, those bodies not only did not collect the relevant data, they did not even try to design valid methodologies for collecting the data.

At the very least, the competent authorities in the EU Member States should have been required to collect, in a systematic and comparable way, reliable information on the outcomes of the passing on of (confirmed) "hits". Given that they have not done so – and that the Commission and the Member States have not even tried to establish reliable systems for this – **there is no insight into how many of the (confirmed) "hits" actually, concretely contributed to the fight against PNR-relevant offences.**

(c) An attempt to apply the tests to the different types of matches

Given that the European Commission and the EU Member States have failed to provide the hard data that are needed to properly assess the effectiveness of the PNR Directive, I too cannot properly or fully assess that – although, given that the onus in this respect lies squarely on the Commission and the Member States, the failure by them to provide this evidence is sufficient to conclude that the directive violates the EU Charter of Fundamental Rights.

However, I believe that even in spite of the hard data, some pertinent observations can still be made on the different types of processing – on the different matches that are carried out – under the PNR Directive and on the lawfulness, suitability, effectiveness and proportionality of that processing. In these, I draw on my analyses in section 4, in particular those relating to the different kinds of matches, set out in sub-section 4.9.

In my opinion, the following can usefully be observed as regards the lawfulness, suitability, effectiveness and proportionality of the different kinds of matches:

(ca) *Re* Matching of basic identity data in PNRs against the identity data of "known" formally wanted persons:

(cb) *Re* Matching of basic identity data in PNRs against the identity data of "known" "persons of interest":

Paradoxically, PNR data are both excessive for the purpose of basic identity checks (of both kinds mentioned above), by containing extensive data that are not needed for such checks, and insufficient ("too limited"), in particular in relation to intra-Schengen flights, by not (always) including the dates of birth of the passengers.

In other words, while API data or data from machine-readable travel documents (MRTD) could be suitable and proportionate to the purpose of basic identity checks, full PNR data are disproportionate to it.

(cc) *Re* Matching of PNR Data against data on lost/stolen/fake credit cards and lost/stolen/fake identity or travel documents:

The matching of PNR data against Interpol's Stolen and Lost Travel Document database is somewhat of a residual check because that database is also already made available to airlines through Interpol's "I-Checkit" facility. This raises doubts as to the necessity of those checks.

(cd) *Re* Matching of PNR data against other, unspecified, supposedly relevant (in particular national) databases:

The vagueness of the phrase "relevant databases" in Article 6(3)(a) of the PNR Directive and the apparently wide discretion granted to Member States to allow matching against all sorts of unspecified data sets is incompatible with the Charter of Fundamental Rights and the European Convention on Human Rights. It means that the application of the law is not clear or foreseeable to those affected – i.e., the provision is not "law" in the sense of the Charter and the Convention (and EU law generally) – and that the laws can be applied in an arbitrary and disproportionate manner.

(ce) *Re* Matching of PNR data against lists of "suspicious travel agents", "suspicious routes", etc.:

No proper prosecuting or judicial authority could declare travellers to be a formal suspect – let alone to charge, prosecute or convict a traveller – on the basis of a match against the above-mentioned, typical, simple "suspicious" elements alone. This raises serious doubts as to the necessity and proportionality of those checks.

(cf) *Re* Matching of data in the PNRs against more complex "pre-determined criteria" or profiles:

In these matches, the PNR database is being used as a test laboratory for advanced data mining technologies using sophisticated, self-learning/AI-based algorithms. Yet they are inherently and irredeemably flawed:

- because the "base-rate" for the PNR data mining is so high (in the region of 500 million people) and the incidence of terrorists and serious criminals within this population so relatively low, algorithm/AI-based profiling is likely to result in tens and possibly hundreds of thousands of "false positives": individual air passengers who are wrongly labelled to a be person who "may be" involved in terrorism or other serious crime;
- the provisions in the PNR Directive that stipulate that no sensitive data may be processed, and that individual decisions and matches may not be "solely based on" sensitive aspects of the individuals concerned do not protect those individuals from discriminatory outcomes of the profiling;
- the algorithm/AI-based outcomes of the processing are almost impossible to challenge because those algorithms are constantly dynamically changed ("improved" through self-learning) and therefore in effect impossible to fully comprehend even by those carrying out the analyses/risk assessments; and
- the outputs and outcomes of the algorithm/AI-based profiling and data mining and matching are not subject to proper scientific testing or auditing, and extremely unlikely to made subject to such testing and auditing.

In sum:

- **full PNR data are disproportionate to the purpose of basic identity checks;**
- **the necessity of the PNR checks against Interpol's Stolen and Lost Travel Document database is questionable;**
- **the matches against unspecified national databases and "repositories" are not based on foreseeable legal rules and are therefore not based on "law";**
- **the necessity and proportionality of matches against various simple, supposedly "suspicious" elements (tickets bought from a "suspicious" travel agent; "suspicious" travel route; etc.) is highly questionable; and**
- **the matches against more complex "pre-determined criteria" and profiles are inherently and irredeemably flawed and lead to tens and possibly hundreds of thousands of innocent travellers wrongly being labelled to be a person who "may be" involved in terrorism or serious crime, and are therefore unsuited (D: *ungeeignet*) for the purpose of fighting terrorism and serious crime.**

5.3 Overall conclusions

The PNR Directive and the generalised, indiscriminate collection of personal data on an enormous population – all persons flying to or from, and the vast majority of people flying within, the EU – that it facilitates (and intends to facilitate) is part of a wider attempt by the European Union and the EU Member States to create means of mass surveillance that, in my opinion, fly in the face of the case-law of the Court of Justice of the EU.

In trying to justify the directive and the processing of personal data on hundreds of millions of individuals, the vast majority of whom are indisputably entirely innocent, the European Commission and the Member States not only do not produce relevant, measurable and peer-reviewable data, they do not even attempt to provide for the means to obtain such data.

Rather, they apply "measures" of effectiveness that are not even deserving of that name: the wide use of the data and the "belief" of those using them that they are useful.

If proper tests are applied (as set out in sub-section 5.2(a), above), the disingenuousness of the "justifications" becomes clear: the claims of effectiveness of the PNR Directive (and the Dutch PNR Law) are based on sand; in fact, as the Dutch researchers rightly noted:

> **"There are no quantitative data on the way in which [and the extent to which] PNR data have contributed to the prevention, detection, investigation and prosecution of terrorist offences and serious crime."**

The Commission and the Member States also ignore the "high risks" that the tools used to "identify" individuals who "may be" terrorists or serious criminals entail. This applies in particular to the use of algorithm/AI-based data mining and of profiles based on such data mining that they want to massively increase.

If the Court of Justice were to uphold the PNR Directive, it would not only endorse the mass surveillance under the directive as currently practised – it would also give the green light to the massive extension of the application of (so far less used) sophisticated data mining and profiling technologies to the PNR data without regard for their *mathematically inevitable* serious negative consequences for tens and possible hundreds of thousands of individuals.

What is more, that would also pave the way to yet further use of such (dangerous) data mining and profiling technologies in relation to other large population sets (such as all users of electronic communications, or of bank cards). Given that the Commission has stubbornly refused to enforce the *Digital Rights Ireland* judgment against Member States that continue to mandate retention of communications data, and is in fact colluding with those Member States in actually seeking to re-introduce mandatory communications data retention EU wide in the e-Privacy Regulation that is currently in the legislative process, this is a clear and imminent danger.

The hope must be that the Court will stand up for the rights of individuals, enforce the Charter of Fundamental Rights, and declare the PNR Directive (like the Data Retention Directive) to be fundamentally in breach of the Charter.

- o – O – o -

Douwe Korff (Prof.)
Cambridge (UK)
November 2021

Attachment 1: Crimes subject to the PNR Directive ("PNR-relevant offences")

As explained in the body of this paper, the overall aim of the PNR Directive is to prevent, detect, investigate and prosecute individuals involved in "terrorist offences" or in other "serious crime"; and the aim of the checking of PNR data by PIUs is to "identify" individuals who may be such persons. The relevant offences are more specifically defined in, respectively, Articles 3 – 12 of Directive (EU) 2017/541 (replacing Articles 1 – 4 of Council Framework Decision 2002/475/JHA) and in Annex II to the PNR Directive. These list the offences set out below. Note however that the PNR Directive only applies to these offences provided that they are "*punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State.*" (Article 3(9)).

I. Terrorist offences as listed in Directive (EU) 2017/541:

TITLE II

TERRORIST OFFENCES AND OFFENCES RELATED TO A TERRORIST GROUP

Article 3

Terrorist offences

1. Member States shall take the necessary measures to ensure that the following intentional acts, as defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organisation, are defined as terrorist offences where committed with one of the aims listed in paragraph 2:

(a) attacks upon a person's life which may cause death;

(b) attacks upon the physical integrity of a person;

(c) kidnapping or hostage-taking;

(d) causing extensive destruction to a government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss;

(e) seizure of aircraft, ships or other means of public or goods transport;

(f) manufacture, possession, acquisition, transport, supply or use of explosives or weapons, including chemical, biological, radiological or nuclear weapons, as well as research into, and development of, chemical, biological, radiological or nuclear weapons;

(g) release of dangerous substances, or causing fires, floods or explosions, the effect of which is to endanger human life;

(h) interfering with or disrupting the supply of water, power or any other fundamental natural resource, the effect of which is to endanger human life;

(i) illegal system interference, as referred to in Article 4 of Directive 2013/40/EU of the European Parliament and of the Council [19] in cases where Article 9(3) or point (b) or (c)

of Article 9(4) of that Directive applies, and illegal data interference, as referred to in Article 5 of that Directive in cases where point (c) of Article 9(4) of that Directive applies;

(j) threatening to commit any of the acts listed in points (a) to (i).

2. The aims referred to in paragraph 1 are:

(a) seriously intimidating a population;

(b) unduly compelling a government or an international organisation to perform or abstain from performing any act;

(c) seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation.

Article 4

Offences relating to a terrorist group

Member States shall take the necessary measures to ensure that the following acts, when committed intentionally, are punishable as a criminal offence:

(a) directing a terrorist group;

(b) participating in the activities of a terrorist group, including by supplying information or material resources, or by funding its activities in any way, with knowledge of the fact that such participation will contribute to the criminal activities of the terrorist group.

TITLE III

OFFENCES RELATED TO TERRORIST ACTIVITIES

Article 5

Public provocation to commit a terrorist offence

Member States shall take the necessary measures to ensure that the distribution, or otherwise making available by any means, whether online or offline, of a message to the public, with the intent to incite the commission of one of the offences listed in points (a) to (i) of Article 3(1), where such conduct, directly or indirectly, such as by the glorification of terrorist acts, advocates the commission of terrorist offences, thereby causing a danger that one or more such offences may be committed, is punishable as a criminal offence when committed intentionally.

Article 6

Recruitment for terrorism

Member States shall take the necessary measures to ensure that soliciting another person to commit or contribute to the commission of one of the offences listed in points (a) to (i) of Article 3(1), or in Article 4 is punishable as a criminal offence when committed intentionally.

Article 7

Providing training for terrorism

Member States shall take the necessary measures to ensure that providing instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques, for the purpose of committing, or contributing to the commission of, one of the offences listed in points (a) to (i) of Article 3(1), knowing that the skills provided are intended to be used for this purpose, is punishable as a criminal offence when committed intentionally.

Article 8

Receiving training for terrorism

Member States shall take the necessary measures to ensure that receiving instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques, for the purpose of committing, or contributing to the commission of, one of the offences listed in points (a) to (i) of Article 3(1) is punishable as a criminal offence when committed intentionally.

Article 9

Travelling for the purpose of terrorism

1. Each Member State shall take the necessary measures to ensure that travelling to a country other than that Member State for the purpose of committing, or contributing to the commission of, a terrorist offence as referred to in Article 3, for the purpose of the participation in the activities of a terrorist group with knowledge of the fact that such participation will contribute to the criminal activities of such a group as referred to in Article 4, or for the purpose of the providing or receiving of training for terrorism as referred to in Articles 7 and 8 is punishable as a criminal offence when committed intentionally.

2. Each Member State shall take the necessary measures to ensure that one of the following conducts is punishable as a criminal offence when committed intentionally:

(a) travelling to that Member State for the purpose of committing, or contributing to the commission of, a terrorist offence as referred to in Article 3, for the purpose of the participation in the activities of a terrorist group with knowledge of the fact that such participation will contribute to the criminal activities of such a group as referred to in Article 4, or for the purpose of the providing or receiving of training for terrorism as referred to in Articles 7 and 8; or

(b) preparatory acts undertaken by a person entering that Member State with the intention to commit, or contribute to the commission of, a terrorist offence as referred to in Article 3.

Article 10

Organising or otherwise facilitating travelling for the purpose of terrorism

Member States shall take the necessary measures to ensure that any act of organisation or facilitation that assists any person in travelling for the purpose of terrorism, as referred to in

Article 9(1) and point (a) of Article 9(2), knowing that the assistance thus rendered is for that purpose, is punishable as a criminal offence when committed intentionally.

Article 11

Terrorist financing

1. Member States shall take the necessary measures to ensure that providing or collecting funds, by any means, directly or indirectly, with the intention that they be used, or in the knowledge that they are to be used, in full or in part, to commit, or to contribute to the commission of, any of the offences referred to in Articles 3 to 10 is punishable as a criminal offence when committed intentionally.

2. Where the terrorist financing referred to in paragraph 1 of this Article concerns any of the offences laid down in Articles 3, 4 and 9, it shall not be necessary that the funds be in fact used, in full or in part, to commit, or to contribute to the commission of, any of those offences, nor shall it be required that the offender knows for which specific offence or offences the funds are to be used.

Article 12

Other offences related to terrorist activities

Member States shall take the necessary measures to ensure that offences related to terrorist activities include the following intentional acts:

(a) aggravated theft with a view to committing one of the offences listed in Article 3;

(b) extortion with a view to committing one of the offences listed in Article 3;

(c) drawing up or using false administrative documents with a view to committing one of the offences listed in points (a) to (i) of Article 3(1), point (b) of Article 4, and Article 9.

Note also the following provision from Title IV:

Article 14

Aiding and abetting, inciting and attempting

1. Member States shall take the necessary measures to ensure that aiding and abetting an offence referred to in Articles 3 to 8, 11 and 12 is punishable.

2. Member States shall take the necessary measures to ensure that inciting an offence referred to in Articles 3 to 12 is punishable.

3. Member States shall take the necessary measures to ensure that attempting to commit an offence referred to in Articles 3, 6, 7, Article 9(1), point (a) of Article 9(2), and Articles 11 and 12, with the exception of possession as provided for in point (f) of Article 3(1) and the offence referred to in point (j) of Article 3(1), is punishable.

II. Serious offences as listed in Annex II to the PNR Directive:

ANNEX II

List of offences referred to in point (9) of Article 3

1. participation in a criminal organisation,
2. trafficking in human beings,
3. sexual exploitation of children and child pornography,
4. illicit trafficking in narcotic drugs and psychotropic substances,
5. illicit trafficking in weapons, munitions and explosives,
6. corruption,
7. fraud, including that against the financial interests of the Union,
8. laundering of the proceeds of crime and counterfeiting of currency, including the euro,
9. computer-related crime/cybercrime,
10. environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties,
11. facilitation of unauthorised entry and residence,
12. murder, grievous bodily injury,
13. illicit trade in human organs and tissue,
14. kidnapping, illegal restraint and hostage-taking,
15. organised and armed robbery,
16. illicit trafficking in cultural goods, including antiques and works of art,
17. counterfeiting and piracy of products,
18. forgery of administrative documents and trafficking therein,
19. illicit trafficking in hormonal substances and other growth promoters,
20. illicit trafficking in nuclear or radioactive materials,
21. rape,
22. crimes within the jurisdiction of the International Criminal Court,
23. unlawful seizure of aircraft/ships,
24. sabotage,
25. trafficking in stolen vehicles,
26. industrial espionage.

- o – O – o -

Attachment 2: The Commission's case studies analysed

In three sections in the staff working document that accompanied the report of the European Commission on the review of the PNR Directive, a total of 13 "case studies" are provided that are intended to illustrate aspects of the operation of the directive. In this attachment, we reproduce the case studies verbatim in sections I – III (with case numbers added), and briefly comment on each of them (in *italics*). In section IV, we provide a very brief analysis. We draw on the cases and comments, and set out the more general conclusions reached on the basis of our analysis, in the body of this paper.

III. Case studies illustrating the different means of processing PNR data:

(Staff working document, section 5.1, case numbers added)

Case number 1: A fugitive convicted to a six-year prison sentence for drug-related offences was wanted by the authorities. The processing of PNR data, received by the Passenger Information Unit at least 24 hours before the flight departure, allowed to notify the relevant authority well in advance and to prepare for action before the arrival of the airplane, coming from a non-EU country. The individual was arrested immediately after arrival and brought before a judge.

Comment: This is an example of an apparently straight-forward match of PNR data against lists of fugitive convicts. It is highly likely that basic API data would have sufficed to identify the individual.

Case number 2: In another example, four individuals belonging to an organised crime group were wanted for kidnapping and attempted murder of an adolescent, aged 17. The video recording of this violent assault was widely shared on social media and caused widespread shock. The processing of PNR data established that one of the suspects was on a plane arriving from Asia. The man was arrested upon arrival. The investigators also found his car in the airport carpark. The analysis of the car's navigation system led to the discovery of the victim's body, abandoned 200 km away from the crime scene.

Comments: This would also appear to be an example of a fairly straight-forward matching of the suspect's basic identity data. Presumably, if the suspect's identity was indeed known already, his car would also have been found without the PNR data, although perhaps only later.

Case number 3: A Passenger Information Unit transferred information regarding suspicious travel patterns of persons linked to a specific company to a unit dealing with organised crime. On the basis of the information provided by the Passenger Information Unit, the organised crime unit launched an investigation into the activities of individuals previously unknown to law enforcement authorities. The investigation revealed their involvement in money laundering and other international economic crimes.

Comment: This case suggests that the PIUs are either provided with examples of what constitute "suspicious travel patterns", or somehow discern such patterns themselves. But of course, it does not indicate how often innocent individuals were "identified" as being possibly involved in terrorism or serious crimes on the basis of such patterns, or what happened with them.

Case number 4: In one Member State, convicted sex offenders must notify their intention to travel abroad and may be refused authorisation if the destination is considered to present a risk. A disproportionate number of convicted offenders declared travels to Dubai. However, the processing of PNR data showed that these offenders booked further flights to destinations to which travel would not have been authorised. The processing also enabled the authorities to establish that all the bookings were made by the same employee of a travel agency. Without PNR processing, the authorities would have not been able to establish the link between the passengers and the travel agency and would not have known about their final destination.

Comment: This case suggests that notifications of intended travel, submitted by convicted sex offenders to the authorities of the Member State in question, are retained and analysed. The case description suggests that the link to the particular travel agency (and the particular employee of that agency) and the details of the onward flights were discovered by the Member State's PIU from the PNRs. It is of course good that this group of offenders (and their facilitator in the agency) was caught – but it also shows that they were not very sophisticated at hiding their plans. Other offenders will have been able to buy a ticket only to Dubai, from a different travel agency, and only once in Dubai an onward flight from a local agency, or directly from the airline providing the onward flight (the PNRs of which would not be sent to the PIUs in the EU as it would not be a flight to, from or within the EU). Still, this can be said to be a case showing that information on the travel agency from which tickets are bought can be useful in some cases. The same will apply to information on any bank card used (although more sophisticated criminals will be aware that such matters will be watched and can evade detection by these means by not using the same agent several times, or a suspect bank card).

Case number 5: In another case, PNR processing revealed that three children were travelling unaccompanied outside Europe. There was no information on who should receive them upon their arrival. The authorities of the country of arrival were alerted and carried out a control on the person waiting for the children, who turned out to be a convicted sex offender. Without the processing of PNR data, it would have not been possible to know that the children were travelling unaccompanied and no additional controls would have been carried out.

Comment: The description of the case is not very clear. Were the children travelling from outside the EU to an EU Member State, or the other way around? In any case, would airport or border control agencies really never check on who is meeting a group of minors? Still, this can be said to be a case showing that information on whether certain passengers are unaccompanied minors can be useful in some cases.

Case number 6: The use of pre-determined criteria indicated that an individual might be potentially travelling to a terrorist training camp. An analysis on the persons' travel history revealed that the person had travelled to this destination many times before, while trying to conceal the final destination. The individual's involvement in a violent extremist organisation, responsible for several terrorist attacks, was later confirmed.

Comment: This is one of only two examples given of a case resolved by means of "the use of pre-determined criteria" (the other one is case 11, below). Yet the description of this case, too, is far from clear. The way the case is written up suggests that the person's travel history was only analysed after he or she was "identified", on the basis of "pre-determined criteria", as

"potentially travelling to a terrorist training camp" – but those criteria are neither spelled out nor even broadly indicated. It says precisely nothing about the nature of those criteria or about how they are created, nor about the number of innocent people who are flagged up as possible terrorists on the basis of those criteria, i.e., about the false positive rate.

IV. Case studies illustrating the use of historical data:

(Staff working document, section 5.2, case numbers added)

Case number 7: The police in a Member State was engaged in an ongoing investigation wherein it was gathering evidence to prosecute a suspect accused of human trafficking, in the context of the activities of an organised crime group. To link the suspect with the victims, information about a flight made in 2015 was necessary. As the Passenger Information Unit of that Member State had been established after this date, it made a request to the Passenger Information Unit which was operating in the destination of the relevant flight. The requested Passenger Information Unit was able to transmit flight information that linked the suspect with the victims (all passengers had been booked under one PNR) and provided the necessary evidence against the suspect.

Comment: If the suspect was already accused of human trafficking and the authorities already knew of the specific flight in 2015, it would appear there was already some evidence against him, and the request for historical data was therefore supplementary rather than central. But that aside, this can be said to be a case showing that information on whether certain passengers were flying together can be useful in some cases (although of course, a more clever trafficker would not have booked all the passengers together, resulting in one PNR for all of them; in fact, traffickers, being aware that they are being looked for, often give their victims their tickets without travelling with them).

Case number 8: In another case, two persons were arrested and charged with drug trafficking. Despite the fact that the arrest took place in a public place, when the defendants were exchanging drugs and money, they both denied knowing each other when interrogated. However, the analysis of PNR data established that they had travelled together 20 times during a period of 2 years. They had not only booked the same flights, but also travelled next to one another.

Comment: These were another two rather stupid criminals. Given that they were apparently caught red-handed exchanging drugs and money (or drugs for money?), they would not have escaped conviction. More important, the fact that they had travelled together 20 times within 2 years could have been established by means of API data – there was no need for the further data contained in PNRs in this case.

Case number 9: A Passenger Information Unit was requested to provide travel information related to a person suspected to have been involved in ISIS activities in Syria before being arrested in another Member State. Intelligence available on the suspect pointed to a rich travel history around Europe. The analysis of PNR data allowed to trace back the movements of this individual between several Member States and to identify potential co-travellers. This information played a crucial role in this specific investigation and provided valuable insights into new travel patterns of ISIS members returning to Europe.

Comment: In this case, too, there was apparently already evidence against the suspect. The analysis of the historical PNR data appears to have been aimed at (i) establishing "[new] travel patterns" and (ii) identifying "potential [?] co-travellers". Presumably, the latter meant marking all passengers on all the flights the suspect had been on in the last five years as "potential" fellow ISIS members, even though the vast majority of them will have been entirely innocent.

Case number 10: An individual had been wanted by law enforcement in relation to serious drug offences for more than 10 years. Intelligence indicated that the individual was a frequent traveller to other European countries, but no details of the person's travel history could be identified. Communications data analysis of a telephone number attributed to the individual revealed when their phone was in certain countries. Analysis of passenger data for flights to and from those locations on specified days revealed a single otherwise unknown individual whose travel destination matched the location of the mobile telephone. Analysis of this individual's PNR revealed a previously unknown identity, email address and residential address. This intelligence-led investigative work led to the person's arrest. Without the use of historical PNR data, this arrest would have not been possible.

Comment: This was a clever use of matching different datasets, i.e., of a data set showing a list of locations for certain dates, and of a data set of flights between those locations on (or around) those dates. But this could have been done with API data: there was no need, in this case, for any of the additional data found in PNRs. (And of course, more sophisticated criminals know to use "burn phones" [mobile phones that are thrown away after single use] and would use more than one false identification document.)

Case number 11: The use of pre-determined criteria, developed on the basis of historical data, enabled the arrest of a passenger upon the arrival from Airport X with 4kg of heroin. The previously unknown passenger's PNR contained data elements that corresponded to pre-determined criteria created after the arrest of other drug smugglers.

Comment: This is the second of only two examples given of a case resolved by means of "the use of pre-determined criteria" (the other one is case 6, above). Unfortunately, the description is so cryptic as to be meaningless as a "case study". It merely says that PNR data on apprehended drug smugglers are used to create "pre-determined criteria", and that when a new person's PNR data match these "pre-determined criteria", that person is then "identified" as a person likely to be involved in drug smuggling – and (it seems at least in this case) arrested (merely?) on this basis, i.e., because his PNR data match the criteria. Once again, there is no information on whether any – or if any, how many – other, innocent people's PNRs were flagged up on this basis, and whether they were all arrested, or what happened after that.

V. Case studies illustrating the use of PNR data collected on intra-EU flights:

(Staff working document, section 5.2, case numbers added)

Case number 12: A third country national residing in one Member State was prohibited from entering the territory of another Member State because of links with a terrorist organisation. It was only thanks to the processing of PNR data that the individual's presence on a plane was discovered by the authorities. The person was intercepted immediately after arrival and sent back on the same day.

Comment: This is yet another example of an apparently straight-forward match of PNR data against a lists – in this case, of persons in one EU Member State who are prohibited from entering the territory of another Member State (cf. cases 1 and 2, above). Again, it is highly likely that basic API data would have sufficed to identify the individual.

Case number 13: Based on the information provided by the Passenger Information Unit of Member State A, related to a match obtained by comparing PNR data with the SIS, the Border Police of Member State B was alerted while a person of interest was travelling from Member State A and the individual was arrested in compliance with an European Arrest Warrant issued by Member State C. As this was an intra-EU flight, passengers were not subject to border controls. Only the collection of PNR data made it possible to identify the target and conduct the arrest.

Comment: This too is an example of an apparently straight-forward match of PNR data against a lists or database – in this case, SIS (cf. cases 1, 2 and 12, above). Again, it is highly likely that basic API data would have sufficed to identify the individual.

VI. Brief analysis

The "case studies" are very limited. They consist of just thirteen selectively chosen examples of "true positive" results from the processing of PNR data on some 500 million people. They say nothing about false positives or false negatives, or the suitability, effectiveness or proportionality of the processing generally.

Still, the following can be gleaned from this selective selection:

- In almost half of the cases (Cases 1, 2, 8, 10, 12 and 13), the cases could have been resolved with the use of API data: there was no need for any of the further, often more revealing data included in full PNRs;
- Some cases show that some data that are not included in API data could be useful in screening passengers, such as:
  - information on the travel agency from which tickets are bought (Case 4);
  - information on whether a passenger is an unaccompanied minor (Case 5);
  - information on whether certain passengers are flying as a group (meaning they share the same PNR) (Case 7);

  and to this could be added:

  - information on the amount of luggage checked in by a traveller;[277] and
  - information on any bank card used.

  Note that the information items noted in the bullet-points above are all "hard" data; they do not require any pattern analysis or any creation of more sophisticated "criteria".

[277] See footnote 6, above.

- There are two cases that are said to have been resolved on the basis of "pre-determined criteria" (Cases 6 and 11). In Case 6, the main element in these criteria appears to have been the suspect's travel history. There may have been other elements such as his nationality (or even ethnicity or religion?)[278] but if there were, those are not revealed. Case 11 is more a description of what the use of "pre-determined criteria entails than a case study. But it makes clear that PNR data on apprehended drug smugglers are used to create "pre-determined criteria", and that when a new person's PNR data match these "pre-determined criteria", that person is then "identified" as a person likely to be involved in drug smuggling – and (it seems at least in this case) arrested (merely?) on this basis, i.e., because his PNR data match the criteria.
- In one further case (Case 9), analysis of a known suspect's historical PNR data appears to have been aimed at (i) establishing "[new] travel patterns" and (ii) identifying "potential [?] co-travellers". Presumably, the latter meant marking all passengers on all the flights the suspect had been on in the last five years as "potential" fellow ISIS members, even though the vast majority of them will have been entirely innocent.

  The main point to make about these latter two sets of cases (Cases 6, 9 and 11) is that in none of them does the staff working document provide any information on whether any – or if any, how many – other, innocent people's PNRs were flagged up on the basis of the "travel patterns" or "pre-determined criteria" mentioned, and whether they were all prevented from flying, or arrested, or what happened after that.

Overall, the "case studies" (insofar as they show anything) show that:

(i) in many cases API data will suffice to achieve the aims of the PNR Directive, without the need for further PNR data;

(ii) some additional "hard" data could usefully be added to the API data; and

(iii) the "pre-determined criteria" are created on the basis of patterns observed in the PNR data, apparently mainly patterns in travel history or in "typical" amounts of luggage checked in by passengers for certain kinds of trips.

However, they reveal absolutely nothing about:

(iv) the precise nature of the pattern analyses;

(v) the numbers (or percentages) of individuals who were "identified" on the basis of the above tests as warranting "further examination", but who turned out (upon such further examination, by the relevant "competent authorities") to not be terrorists or serious criminals, or indeed entirely innocent – but who are nevertheless very likely to have been significantly negatively affected by the "hit". Case 9 in particular suggests that there must be significant numbers of such **false positives**;

[278] See the discussion of the use of sensitive personal data in section 4, sub-section 4.8(b), above.

(vi) the numbers (or percentages) of actual terrorists or serious criminals who were not "identified" on the basis of the above tests as warranting "further examination", and therefore allowed to fly and not arrested on the basis of the PNR checks, i.e., of the numbers (or percentages) of **false negatives**.

I discuss the nature of the pattern analyses in section 4.9 of the opinion, and the other core issue – the suitability, effectiveness and proportionality of the PNR checks – in section 5 of the opinion. In the latter section, I note that not only do the Commission report and the staff working paper throw no light on these crucial issues, but also that the discussions at the July 2021 Court hearing basically missed the point in the latter regard and in particular the question of what constitutes "true", respectively "false positives".

- o – O – o -

Attachment 3: The use of bulk data by the UK intelligence agencies

Excerpt from Douwe Korff & Ian Brown, The inadequacy of UK data protection law – *Part Two: UK surveillance*, November 2020, section 2.3, *How the [e-communications] data [obtained through the UK-USA bulk interception programme] are used*, with minor edits (and with paragraphs not relevant to PNR data removed, as indicated by "…". Original footnotes.)

1.3.1 Introduction

A 2015 UK House of Commons Intelligence and Security Committee report (on bulk interception of electronic communications by the UK's Government Communications Headquarters (GCHQ) notes two elements to GCHQ's bulk interception programme:[279]

> GCHQ's bulk interception capability is used either to investigate the communications of individuals already known to pose a threat, or to generate new intelligence leads, for example to find terrorist plots, cyber attacks or other threats to national security.

Below, we briefly describe the (overlapping) parts to the programme, while noting likely new technical developments in particular in relation to the second part (the "new threat" detection).

1.3.2 Monitoring of individuals already "known" to pose a threat

As the UK NGO *Open Rights Group* (ORG) explains, the first part of the programme is:[280]

> an "investigative tool", targeted at "specific identifiers relating to a known suspect" to be analysed by intelligence operatives.

The parliamentary Intelligence and Security Committee has stated these "known suspects" or "known threats" may be targeted in the UK by means of more traditional communication interception,[281] but the data collected in bulk from the Internet bearers are also filtered to find information on such known suspects or threats, by means of "simple selectors":[282]

> Any communications which match the specific 'simple selectors' are automatically collected. All other communications are automatically discarded.[283] …

---

279 UK House of Commons' Intelligence and Security Committee, Privacy and Security: A modern and transparent legal framework (HC 1075), 12 March 2015 (hereafter, "**the ISC Report**"), p. 28, available at: http://isc.independent.gov.uk/news-archive/12march2015
GCHQ is the UK's Government Communications Headquarters, responsible for collecting signals intelligence. It works closely with the US National Security Agency (NSA) in extracting e-communications data in bulk from the undersea cables through which much of the European Internet traffic flows and that pass through the UK (as described in *Part Two* of the Korff/Brown submission.

280 Open Rights Group, Collect It All: GCHQ and mass surveillance, 2015 ("**the ORG report**"), para. 17, available at:
https://www.openrightsgroup.org/publications/collect-it-all/

281 ISC report, p. 3; cf also para. 56, on p. 27.

282 *Idem*, para. 61. The statistics in this paragraph have been obscured, hence our omission of the relevant – to the non-privileged reader, useless – sentence.

283 GCHQ also collect all the Communications Data associated with these communications (described as 'Related Communications Data' in RIPA) before extracting that which is most likely to be of intelligence value. We return to this issue in Chapter 6. [original footnote]

1.3.3 Identifying new threats and previously unknown persons "of interest"

i. Identifying new threats through "complex selectors" and "selection rules"

This part of the programme is described in the ISC report, with significant redactions, as follows:[284]

> Another major processing system by which GCHQ may collect communications is ***, **where GCHQ are looking to match much more complicated criteria with three or four elements**, for example.[285] Unlike the simple selectors used in the first process, this technique requires ***.
>
> This process operates across a far smaller number of bearers – GCHQ choose just *** of the bearers out of those they can theoretically access.[286] **These bearers are not chosen at random: they are deliberately targeted as those most likely to carry communications of intelligence interest.** (For example, GCHQ are currently targeting bearers likely to be carrying communications of ***.)
>
> **As a first step in the processing under this method, ***. *** the system applies a set of 'selection rules'.** As of November 2014, there were *** selection rules. ***. Examples of these initial selection rules are:
>
> - include ***;
> - include ***; and
> - discard communications ***.
>
> As a result of this selection stage, the processing system automatically discards the majority (***) of the traffic on the targeted bearers. The remainder is collected ***. These communications are the ones that GCHQ consider most likely to contain items of intelligence value.
>
> ***.
>
> **GCHQ's computers then perform automated searches using complex criteria (***) to draw out communications of intelligence value.** By performing searches combining a number of criteria, the odds of a 'false positive' are considerably reduced. ***.
>
> While analysts may create **additional bespoke searches based on the complex criteria**, the system does not permit them to search freely (i.e. they cannot conduct fishing expeditions). GCHQ explained: "***".
>
> **The individual communications which match these complex searches** number approximately *** items per day. These **are made available, in list form, to analysts for possible examination and storage** (we consider the criteria for examination later in this chapter).
>
> …

---

284 ISC report, paras. 65 – 73, emphases added, footnotes that simply cross-refer to "Written Evidence – GCHQ", with a date, omitted. All the information is based on this written evidence.

285 GCHQ have a number of other capabilities of this type, including: ***. [original footnote]

286 These are a subset of the same bearers that are accessed under the method already described. [original footnote] We understand the reference to "the method already described" to refer to the filtering by means of simple selectors.

[We note] the claim that "*[b]y performing searches combining a number of criteria, the odds of a 'false positive' are considerably reduced.*" That may be true for clearly specified selectors or rules, e.g., a search for "male AND Muslim AND aged 18 – 28 AND Syrian national" will throw up less false positives than a search that uses only one or a few of these search terms. But as we shall note in the next section, the problem of excessive false positives (and excessive false negatives) cannot be avoided in Big Data datamining operations. In that next section, we will also note that the reference to the analysts not being allowed to "*conduct fishing expeditions*" is misleading in the context of such more sophisticated operations.

ii. Identifying new threats and previously unknown persons "of interest" through more sophisticated data mining

THE BULK DATA

The Bulk communications data

[The ISC report describes the broad sweep of e-communications data, metadata and other associated data collected in bulk, by GCHQ (working closely with the NSA), from bearers in undersea cables that carry the communications of millions of individuals, and the Korff/Brown submission discusses these in some detail, but apart from noting that broad sweep these matters are not relevant to the present paper. However, the next discussion is relevant:]

Additional bulk personal datasets

Apart from collecting communications data and especially metadata in bulk, the UK intelligence agencies also have access to other large bulk personal datasets – although all details about them are redacted in the ISC report:[287]

> In addition to obtaining intelligence through capabilities such as interception, **the Agencies also acquire Bulk Personal Datasets containing personal information about a large number of people.** Bulk Personal Datasets may relate to the following types of information:
>
> [All the details and statistics are obscured]
>
> **The Committee was told that the Agencies may share Bulk Personal Datasets between them where they consider this to be lawful, necessary and proportionate.**
>
> **These datasets vary in size from hundreds to millions of records. Where possible, Bulk Personal Datasets may be linked together so that analysts can quickly find all the information linked to a selector (e.g. a telephone number or ***) from one search query. ***.**

We believe – but of course cannot prove since these details are kept secret – that these additional bulk personal datasets may well relate to financial matters such as bank card transactions, wire transfers or bank account details, travel information (in particular Passenger Name Records or PNRs), local government information such as who is registered at a particular address, etcetera.

---

[287] ISC report, para. 151 and 154 – 156, emphases added, footnote references to undisclosed sources and to "*Written Evidence – GCHQ*" and "*Oral Evidence – SIS*" omitted. [The Secret Intelligence Service (SIS), commonly known as MI6, is the UK's foreign intelligence service, tasked mainly with the covert overseas collection and analysis of human intelligence in support of the UK's national security.]

THE USES OF THE BULK DATA

We have written (together, separately and/or with others) about the use of bulk data collection and use for more than 15 years, in relation to predictive policing,[288] the fight against terrorism,[289] national security[290] and border control/PNR data.[291] We believe that the ISC report in particular fails to note the more problematic uses of the bulk personal data by the UK intelligence agencies, in particular the use of Big Data datamining technologies to "identify" individuals as (possible or probable) terrorists or other threats to national or public security. Below, we briefly note both the acknowledged and the less clearly acknowledged uses of the bulk datasets.

Linking "known" Subjects of Interests and events

SIS explained that the additional bulk personal datasets:[292]

> ... are increasingly used to identify the people that we believe that we have an interest in; and also to identify the linkages between those individuals and the UK that we might be able to exploit. ***.

And GCHQ added that:[293]

> they consider Bulk Personal Datasets to be an increasingly important investigative tool, which they use primarily to 'enrich' information that has been obtained through other techniques:
>
> ***.

"Link analysis" of all the bulk personal datasets – the bulk communications data and the other datasets –can be used to identify and map networks of "known" or suspected terrorists, serious criminals or other bad people. It is by now common in police and forensic investigations, especially in relation to retrospective analysis (checking links between individuals and events that have occurred).[294]

---

288 Ian Brown and Douwe Korff, Privacy and Law Enforcement, study for the UK Information Commissioner, 2004, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3737428

289 Douwe Korff, Protecting the Right to Privacy in the Fight Against Terrorism, Issue Paper of the High Commissioner for Human Rights of the Council of Europe, November 2008, available at: https://rm.coe.int/ref/CommDH/IssuePaper(2008)3

290 E.g., Ian Brown & Douwe Korff, Terrorism and the Proportionality of Internet Surveillance, European Journal of Criminology, March 2009, available at: http://ssrn.com/abstract=1261194

Ian Brown & Douwe Korff, Foreign surveillance: law and practice in a global digital environment, European Human Rights Law Review, 2014(3) (April 2014), available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2521433

291 Douwe Korff & Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards, report prepared for the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) of the Council of Europe, June 2015, available at: https://rm.coe.int/16806a601b

292 ISC report, para. 152, reference to "*Oral Evidence – SIS*" omitted.

293 *Idem*, para. 153, reference to "*Written Evidence – GCHQ*" omitted.

294 See: https://en.wikipedia.org/wiki/Link_analysis

It is however important to add a note of caution. The "*people that [the agencies] believe that [they] have an interest in*" are described in the ISC report (no doubt reflecting the agencies' own terminology) as "**Subjects of Interest**".[295] An "SoI" is defined as: *"an individual investigated by the Agencies because they are suspected of being a threat to national security."*[296] But this is quite far removed from a "suspect" as defined in criminal law, i.e., a person in relation to whom there are reasonable grounds to suspect s/he has committed an offence. In deciding whether to designate a person as an SoI, the intelligence agencies (in the UK as elsewhere) apply a (much) lower standard of evidence.

Being identified as a person with links to an SoI casts the net yet further. It can include, for instance, a person who has on several occasions called, or who on several occasions was called by, an SoI, or who on several occasions was in (roughly) the same location as an SoI, or both. **There is no doubt that many of the individuals whose are noted in a link analysis of an SoI's contacts will be entirely innocent people.** But at least, in such cases based on established facts (calls made, places visited), it will often be possible to exclude such innocent people from further inquiries (and invasions of their privacy and other rights).

Automated processing

[Short section on the use of automated natural language processing software, acoustic (voice biometric) technologies and facial recognition software omitted as not relevant in the context of PNR data. But the next discussion is relevant:]

"Identifying" possible other Subjects of Interest through AI-based datamining

The ISC report acknowledges that the UK intelligence agencies also carry out more sophisticated analyses than the above-mentioned filtering by means of "simple" or "complex selectors" and "selection rules", or by relatively straight-forward "link analysis", by referring to agencies' capacities that:[297]

> involve the Agencies casting their nets wider and analysing large volumes of information, which enable the Agencies also to find **linkages, patterns, associations or behaviours** which might demonstrate a serious threat requiring investigation.

The report is somewhat coy about what this actually entails. It says that:[298]

> **GCHQ's bulk interception capability is used primarily to find patterns in, or characteristics of, online communications which indicate involvement in threats to national security.** The people involved in these communications are **sometimes already known**, in which case valuable extra intelligence may be obtained (e.g. a new person in a terrorist network, a new location to be monitored, or a new selector to

---

295 ISC report, para. 20, on p. 14.

296 *Idem*, footnote 14.

297 *Idem*, para. 18, at ii, on p. 13, emphasis added. The ISC adds to this in brackets that "*[t]hese capabilities nevertheless require some degree of targeting in order to ensure that a human eye only looks at that which is most likely to be of intelligence value.*" We will come to that later in this section. It is of course somewhat ironic that the ISC refers on the one hand to the agencies "casting their nets widely", while at the same time claiming that "they cannot conduct fishing expeditions".

298 *Idem*, para. 90, emphases added.

> be targeted). **In other cases, it exposes previously unknown individuals or plots** that threaten our security which would not otherwise be detected.

And that:[299]

> GCHQ have established that they can analyse [communication data] to find **patterns** in it **that reflect particular online behaviours that are associated with activities such as attack planning**, and **to establish links**. (***.)

These quotes indicate the use of advanced datamining of the bulk personal datasets to identify elements and links between elements that no-one would have thought were relevant or linked in advance.[300] Moreover, the algorithms used in the analyses are increasingly **self-learning**, i.e., constantly dynamically re-generated and refined through loops linking back to earlier analyses, in theory constantly improving the outcome, through "**artificial intelligence**". More specifically, in the search for (further) "SoIs", the software creates constantly self-improving and refining **profiles** against which it matches the massive amounts of data – and in the end, it produces lists of individuals that the algorithm suggests may (possibly or probably) be terrorists, or associates of terrorists.

- o – O – o –

299 *Idem*, para. 130, emphases added.

300 The discussion in the text paraphrases in particular the overview of the issues in Douwe Korff & Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards (footnote 73, above), section I.iii, *The dangers inherent in data mining and profiling*, that itself drew on and referenced the earlier papers listed in footnotes 70 – 72, above.
For further technical and other details and analysis, see ORG report, Part One Chapter Three, Putting mass surveillance to use, in particular section 3.4, *Additional issues with processing*. This part of the report is also separately available in pdf at:
https://www.openrightsgroup.org/app/uploads/2020/03/03-Part_One_Chapter_Three-Analytics_and_usage.pdf