MAX PLANCK INSTITUTE
FOR THE STUDY OF
CRIME, SECURITY AND LAW

MPI-CSL
WORKING PAPERS
2023 | 06

The Future of the European Security Architecture

A Debate Series

Evelien Brouwer • Elspeth Guild • Stefan Salomon • Christian Thönnes (editors)

Electronic copy available at: https://ssrn.com/abstract=4547775

Evelien Brouwer, Elspeth Guild, Stefan Salomon,
Christian Thönnes (*Editors*)

The Future of the European Security Architecture

A Debate Series

https://verfassungsblog.de/category/debates/pnr-debate-series/

Universiteit van Amsterdam

ACES
Amsterdam Centre for European Studies

Max Planck Institute for the Study of Crime, Security and Law

Queen Mary University of London
School of Law

Global Digital Cultures

Montaigne Centre

Electronic copy available at: https://ssrn.com/abstract=4547775

Imprint

2023
Max Planck Institute for the Study of Crime, Security and Law
Günterstalstraße 73, 79100 Freiburg im Breisgau

Published under CC-BY-SA 4.0 Germany License
https://creativecommons.org/licenses/by-sa/4.0/deed.de

Electronic copy available at: https://ssrn.com/abstract=4547775

Foreword

Picture this: you want to travel with your family to a friend's wedding in New York. Three days before your flight is scheduled to depart, you are informed by the US embassy in your country that your electronic travel authorisation has been cancelled. The following day, you queue at the US embassy to apply for a visa. In the interview, the consular officer tells you that your travel authorisation has been revoked because the 'algorithm' had identified a security threat. The consular officer says that she does not know what exactly triggered the algorithm, but she presumes that it might be people you have been in contact with or places you have travelled to, or a pattern in the relation between these two or other factors that the 'algorithm' discovered. She tells you that the security officer, in order to swiftly assess your case and, through a manual review of the algorithmic recommendation, rule out that you pose a threat to national security, needs your past 15 years of travel history, as well as the names and contact details of all people in your network. Although this example is drawn from the security apparatus in the US[1], similar scenarios could soon materialise in the European Union, too.

This volume is the outcome of an online debate series, we (along with our affiliated institutions) hosted together with Verfassungsblog.[2] It is dedicated to *Ligue des droits humains*[3] – a case in which the Court of Justice of the European Union (CJEU) decided on the fate of one of the main drivers of this development: the Directive on on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (in short: PNR Directive).[4] The PNR Directive, being one of the first major EU-wide examples of predictive policing, is not just interesting in itself. We believe it merits more attention because it exemplifies the emergence and gradual consolidation of a new security architecture in Europe.

[1] See Weizman, The algorithm is watching you, London Review of Books, 19 February 2020, https://www.lrb.co.uk/blog/2020/february/the-algorithm-is-watching-you, last accessed: 26 June 2023.

[2] All contributions were originally published on Verfassungsblog. They can be accessed here: https://verfassungsblog.de/category/debates/pnr-debate-series/, last accessed: 26 June 2023. We are especially grateful to Marlene Straub for facilitating this debate series.

[3] CJEU, Case C-817/19 *Ligue des droits humains* [21 June 2022].

[4] Directive (EU) 2016/681, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0681, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

A new type of security: from suburbia to high rise

Two decades ago, Europe's security architecture resembled a middle-class suburban neighbourhood, where plots were neatly divided from the neighbouring properties and each family dwelled in a separate house. These houses strongly resembled each other but each was planned by a different architect. Likewise, security strategies, institutions, infrastructures, and legal frameworks were, with a few exceptions, siloed along national lines. Cooperation between member states' authorities was, like in suburban neighbourhood committees, occasional and sporadic – the exception to the architectural rule.

The legal framework, institutional cooperation, the role of and reliance on technological instruments to predict and prevent security risks have radically changed over the past 20 years. Today, the European security architecture more resembles a modern high rise. Although its inhabitants dwell in separate apartments, the building has a common infrastructure, a uniform façade, and common leisure areas, such as terraces and gyms. Its inhabitants use biometric data, instead of manual keys, and complex algorithms in lieu of locks – to access the building and to keep out the unwanted. The building's sophisticated security system, as well as the common leisure areas, are managed centrally by an opaque web of actors.

The security architecture in the EU relies on the extensive use of personal data, including biometric data, collected in large-scale, supranational databases, which are rendered interoperable and searchable through modern and potentially self-learning technologies, in order to automatically predict threats to public security. The focus on predicting and preventing potential threats through automated means consolidates a paradigmatic shift of security: targeted reactions to specific threats to public security by national police authorities have been replaced by all-encompassing surveillance practices, which are based on a general suspicion of everyone, and carried out by a web of actors so complex that even specialised scholars have a hard time disentangling it. This complexity is enhanced by the applicability of different data protection regimes and their specific oversight mechanisms.

This results in a transformation of traditional legal notions and a blurring of classical boundaries. Private power is instrumentalised for surveillance purposes by requiring companies to transmit data, which they collect and process for business purposes. Institutional separations between intelligence gathering and operative policing fall, and functional distinctions between internal security and external migration control fade. EU and national

Electronic copy available at: https://ssrn.com/abstract=4547775

security authorities, once strictly divided, fuse into one single interwoven security apparatus. And modern technologies allow for an increasing delegation of legal decision-making powers from humans to machines, thus opening the floodgates for algorithmic discrimination, opacity in legal decision-making and an erosion of the fundamental legitimacy of state action.

The EU Directive on the use of Passenger Name Records (PNR Directive) is at the heart of the emerging European security architecture. It instrumentalises private air carriers for the indiscriminate collection and state-led automated analysis of PNR datasets relating to hundreds of millions of air passengers, in order to look for potentially suspicious patterns. In the name of combating terrorism and serious crimes, it transcends functional separations between prevention and repression. By relying on member states to upgrade and connect their security authorities for cooperative, algorithmic threat detection, it obliges them to adapt their national laws in an area that used to reside firmly and exclusively in the national sphere – public security. The perceived threat of terrorism, it seems, works wonders in transforming formerly distinct national structures into one European high-rise. After all, to combat this threat, the PNR Directive creates a considerable task for European law enforcement: the amount of data collected and analysed is enormous. Schiphol airport in Amsterdam alone, where the conference took place of which this symposium is the outcome, has an annual volume of more than 72 million passengers. And it doesn't stop with air travel: Belgium, for example, has already expanded the PNR Directive's scope to international trains, buses and ferries. Moreover, the ETIAS Regulation[5] and the EU Commission's proposal for a Regulation to combat child sexual abuse material (CSAM)[6] are partly spiritual successors to the PNR Directive: They also seek to predict threats to public security by means of algorithmic profiling and integrate formerly distinct national authorities into one single European security network for that purpose.

Hence, when in Ligue des droits humains, the CJEU decided on the PNR Directive's compatibility with EU law, it simultaneously rendered a landmark decision on the emerging European security architecture.

[5] Regulation (EU) 2018/1240, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1240, last accessed: 26 June 2023.

[6] Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0209, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

Architecture as metaphor and practice

The metaphor of architecture, as Max Steinbeis noted in his Verfassungsblog editorial[7], is nothing new when it comes to describing the EU. Textbooks in EU law widely used the pillars of the Greek temple to illustrate the pre-Lisbon distribution of competences. The metaphor also lends itself to describe the much more messy post-Lisbon system of multi-level governance and the construction of the walls that separate the inside from the outside.[8] Given ever more restrictive asylum policies, observers warn against the construction of a ‘Fortress Europe’.[9]

Architecture, however, is not only a metaphor, but also a practice that both constructs and reconstructs.[10] Architecture as a critical practice also reconstructs and digitally represents the violence wielded by states and companies over bodies, buildings and the environment, and thus renders public and visible what would otherwise remain invisible. Architecture as critical practice thus aims to bring new aesthetic sensibilities to bear upon the political and legal implications of this violence.[11] In a similar vein, an inquiry into the legal scaffolding that enables and restricts the operation of self-learning technologies for data processes, data transfers, and delegation of decision-making powers from humans to machines is able to uncover the material reality of a multi-layered structure of surveillance.

Another aspect of the notion of architecture as practice is the person of the architect. A quick look into the Treaties suggests that the member states, as masters of the Treaties, and the EU legislature design the blueprint of the European security architecture. However, the development of artificial intelligence is driven by private companies, who de facto assume the role of standard setters, given the absence of legal regulation of self-learning technologies at the state and EU level, and EU institutions’ use of privately-developed algorithms.

These two aspects – architecture as critical practice that makes multi-layered surveillance structures visible, and the increasing role of private actors – points to the importance of the

[7] Steinbeis, That’s Just How It’s Built, Verfassungsblog, 24 February 2023, https://verfassungsblog.de/thats-just-how-its-built/, last accessed: 26 June 2023.
[8] Lynch/Barigazzi, EU vows more cash for frontier policing as border fence debate revives, Politico, 10 February 2023, https://www.politico.eu/article/euco-eu-crosses-into-the-border-fence-game-migration/, last accessed: 26 June 2023.
[9] Rankin, EU leaders plan tougher border controls as more people claim asylum, The Guardian, 10 February 2023, https://www.theguardian.com/world/2023/feb/10/eu-leaders-plan-tougher-border-controls-as-more-people-claim-asylum, last accessed: 26 June 2023.
[10] Forensic Architecture, Pushbacks in Melilla: ND and NT V. Spain, accessible via: https://forensic-architecture.org/investigation/pushbacks-in-melilla-nd-and-nt-vs-spain, last accessed: 26 June 2023.
[11] Forensic Architecture (ed), Forensis (Sternberg Press 2014).

Electronic copy available at: https://ssrn.com/abstract=4547775

judiciary, which has to mould the use of new technologies and power relations into existing legal norms and doctrines that may be ill-fitting. The CJEU has assumed an important role by obliging member states in a series of landmark judgments and opinions – Schrems I[12] and II[13], and Opinion 1/15[14], for instance – to make far reaching changes to the existing security architecture. In the case of *Ligue des droits humains*, the CJEU, again, requires member states to make changes to the security architecture they built.

Our debate series: Taking Ligue des droits humains as a point of departure

Ligue des droits humains formed the background to a two-day conference[15], which took place at the University of Amsterdam from 23 to 24 February 2023. During the conference, we set out to take Ligue des droits humains as a point of departure for discussing the wide-ranging effects and problems of the emerging European security architecture. The objective of the conference was to analyse, from a multi-disciplinary perspective, how fundamental rights and other rule of law principles, such as the accountability of involved actors and contestability of legal decisions, can be upheld in the context of a preventive security paradigm that relies on massive collection and analysis of personal data by self-learning technologies. More specifically, the aim was to explore how the legal standards set by the CJEU in *Ligue des droits humains* could contribute to upholding fundamental rights, such as the rights to data protection and non-discrimination, ensure accountability, and meaningful legal redress.

Two days of intense debate, of course, only mark a first step towards tackling the products and perils of the emerging European security architecture. With this debate series, we set out to continue and build on our discussions in Amsterdam. As an outcome of the debate series, this volume features the following contributions:

- The first contribution provides an analysis of the broader background of the *Ligue des droits humains* judgement and its implications. *Christian Thönnes and Niovi Vavoula* start the discussion with an analysis of the CJEU's findings on automated predictive threat detection.[16] While the Court established in *Ligue des droits humains* "an

[12] CJEU, Case C-362/14 *Maximilian Schrems v Data Protection Commissioner* [6 October 2015].
[13] CJEU, Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems* [16 July 2020].
[14] CJEU, Opinion 1/15 of the Court [26 July 2017].
[15] See https://aces.uva.nl/content/events/2023/02/the-future-of-the-european-security-architecture.html?origin=NY%2F9hMhAQhOv8%2FEeoPahTA, last accessed: 26 June 2023.
[16] See Thönnes/Vavoula, Automated predictive threat detection after Ligue des Droits Humains, page 12.

Electronic copy available at: https://ssrn.com/abstract=4547775

abundance of procedural safeguards to reign in the potential excesses of automated predictive threat detection", it left open many questions on false positives and the effectiveness of human review when thousands of false positives have to be reviewed. This contribution proceeds to assess the effects of the PNR decision for the European Travel Information and Authorisation System (ETIAS) Regulation and the EU Commission's proposal for a Regulation on combating online child sexual abuse material (CSAM).

- *Janneke Gerards* focuses on a different point of automated data processing, namely the risk of discrimination by machine learning algorithms.[17] In *Ligue des droits humains,* the CJEU was very sceptical of the use of machine learning algorithms for risk profiling and imposed strict conditions on their use, including, among others, that a human being must check the pre-determined criteria that resulted in a 'positive hit'. Gerards argues that this might mean that "the role of a predictive algorithm is effectively taken over by humans", who conduct risk assessments based on their own experiences and stereotyped thinking.
- Any risk profiling based on machine learning requires large amounts of data to train that algorithm so that it would accurately 'predict' future risks. *Didier Bigo and Stefan Salomon* trace back the emergence of the idea that large amounts obtained through mass surveillance programs, especially the mass collection of passengers' data, are an effective tool to prevent future threats.[18] They argue that a preventive security logic emerged in the aftermath of 9/11 and the US war on terror, and eventually transformed PNR collection from a commercial activity into a security tool, which fundamentally changed the work of border guards.
- Other authors elaborate on effective judicial remedies, legal contestability under the new architecture and the complex relation between private and public actors, which is a constitutive feature of the new security architecture. The increasing reliance by governments on bulk collection of data was somewhat counterbalanced by national and European courts, which established legal safeguards that ought to prevent disproportionate government access to personal data. Yet, as *Thorsten Wetzling* cautions in his contribution that focuses on the PNR Directive and the German legal

[17] Gerards, Machine learning and profiling in the PNR system, page 25.
[18] Bigo/Salomon, Passenger Name Records and Security, page 32.

Electronic copy available at: https://ssrn.com/abstract=4547775

framework, the necessity requirement and independent review of data collection are in practice often less robust than they appear in theory.[19]

- A precondition for an effective legal remedy is to know which legal framework applies. The new security architecture is built upon complex legal relations between public and private actors. As different legal frameworks and standards apply to data processing by private actors and public actors, *Elspeth Guild and Tamás Molnár* argue, the exact determination of the applicable legal norms and standards often proves to be a very intricate task.[20]
- One aspect of the principle of legality is legal certainty, taken up by *Amanda Musco Eklund* and *Magdalena Brewczyńska* in their contribution.[21] Eklund and Brewczyńska argue that the complex legal enmeshment of public and private actors means that the individual is no longer confronted only with the power of the state, but with a "network of power created by both the state and non-state actors". This eventually has detrimental effects on the principle of legal certainty and raises broader rule of law concerns in the European security architecture.
- *Evelien Brouwer* focuses on the particular challenges that profiling based on artificial intelligence raises for the right to an effective remedy.[22] How can someone who is refused to embark on a flight, because she has been identified as a risk, challenge the possibly discriminatory nature of the risk assessment without knowing the specific assessment criteria? Despite the legal safeguards set forth by the CJEU in its PNR decision, it will, as Brouwer argues, "remain difficult for both individuals and courts to detect and prove the discriminatory nature of these decisions".
- *Chloé Berthélémy* takes up a different angle on the collaboration between private and public actors in the development of security technologies: the different forms of participation of private actors in the EU's security policies.[23] *Berthélémy* maps the different forms of collaboration that range from coerced, voluntary to proactive 'cooperation' of private actors, and the impact that these have on the principle of legality.

[19] Wetzling, Caution: Safeguards may appear more robust than they are, page 40.

[20] Guild/Molnár, The European Legal Architecture on Security, page 48.

[21] Eklund/Brewczyńska, Foreseeability and the Rule of Law in Data Protection after the PNR judgment, page 54.

[22] Brouwer, Challenging Bias and Discrimination in Automated Border Decisions, page 61.

[23] Berthélémy, EU Privacy and Public-Private Collaboration, page 69.

Electronic copy available at: https://ssrn.com/abstract=4547775

- Aligning a future EU AI regime with international rules and embedding it in a transatlantic regulatory regime, as *Daniel Mügge* points out, are important policy goals of the EU.[24] Fundamental rights limitations, as interpreted by the CJEU in the PNR decision and possibly further expanded in future judgements, may thus "define the outer boundaries of regulatory cooperation in the AI field — no matter how much goodwill there might be to find a compromise with, for example, the USA."

The contributions mirror the range of topics and diversity of perspectives that properly addressing the new security architecture's challenges requires. We believe, however, that the contributions are united in their open-endedness: there is so much left to discuss, so many problems to solve and so many standards to elaborate. We therefore bring this debate to Verfassungsblog in the hope that it will foster an even more multifaceted conversation.

The Editors

[24] Mügge, Squaring the triangle of fundamental rights concerns, page 76.

Electronic copy available at: https://ssrn.com/abstract=4547775

Table of Contents

FOREWORD 3

AUTOMATED PREDICTIVE THREAT DETECTION AFTER LIGUE DES DROITS HUMAINS 12
Christian Thönnes, Niovi Vavoula

MACHINE LEARNING AND PROFILING IN THE PNR SYSTEM 25
Janneke Gerards

PASSENGER NAME RECORDS AND SECURITY 32
Didier Bigo, Stefan Salomon

CAUTION: SAFEGUARDS MAY APPEAR MORE ROBUST THAN THEY ARE 40
Thorsten Wetzling

THE EUROPEAN LEGAL ARCHITECTURE ON SECURITY 48
Elspeth Guild, Tamás Molnár

FORESEEABILITY AND THE RULE OF LAW IN DATA PROTECTION AFTER THE PNR JUDGMENT 54
Amanda Musco Eklund, Magdalena Brewczyńska

CHALLENGING BIAS AND DISCRIMINATION IN AUTOMATED BORDER DECISIONS 61
Evelien Brouwer

EU PRIVACY AND PUBLIC-PRIVATE COLLABORATION 69
Chloé Berthélémy

SQUARING THE TRIANGLE OF FUNDAMENTAL RIGHTS CONCERNS 76
Daniel Mügge

Electronic copy available at: https://ssrn.com/abstract=4547775

Automated predictive threat detection after Ligue des Droits Humains

Christian Thönnes, Niovi Vavoula

On 21 June 2022, the Court of Justice of the European Union (CJEU) released its judgment[25] regarding the compatibility of the EU Directive on Passenger Name Record Data (PNR Directive)[26] with the rights to privacy and personal data protection. *Ligue des droits humains* has already qualified as a landmark decision, where the Court had the opportunity, among other aspects, to provide comprehensive guidelines on how large-scale predictive policing should take place. In so doing, the Court followed in the footsteps of La Quadrature du Net[27], and Opinion 1/15[28], which tackle a relentlessly growing kit of big-data-based security instruments.

In the past few years, various security law instruments (both adopted and proposed) have required automated predictive threat detection instruments, meaning that they automatically sift through massive amounts of data in order to predict potential threats to public security. Given this context, *Ligue des droits humains* could be used as an inspiration for their legal assessment.

Against this backdrop, this contribution aims to first provide an outline of the CJEU's findings in *Ligue des droits humains* on automated predictive threat detection, and then to analyse its implications for two other legal instruments relying on automated predictive threat detection: the Regulation establishing a European Travel Information and Authorisation System (ETIAS)[29] and the Commission's proposal for a Regulation on combating online child sexual abuse material (CSAM).[30] While there remains room for elaboration, *Ligue des droits humains* contains a plethora of relevant standards for future security instruments. This contribution will demonstrate that, both ETIAS and the CSAM proposal, in many regards, clash with these standards.

[25] CJEU, Case C-817/19 *Ligue des droits humains* [21 June 2022].
[26] Directive (EU) 2016/681, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0681, last accessed: 26 June 2023.
[27] CJEU, Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net* [6 October 2020].
[28] CJEU, Opinion 1/15 of the Court [26 July 2017].
[29] Regulation (EU) 2018/1240, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1240, last accessed: 26 June 2023.
[30] Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0209, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

Automated predictive threat detection in Ligue des Droits Humains

The CJEU imposed significant limits on the creation and use of algorithms and other forms of modern technology for security purposes. *Ligue des droits humains* gave the Court the opportunity to do so because the PNR Directive obliges designated national security authorities, so-called Passenger Information Units (PIUs), to automatically process PNR data by comparison, not only against pre-existing databases (Art. 6 (3)(a), but also "pre-determined criteria". The latter are algorithms which, in the Commission's words, contain "search criteria, based on the past and ongoing criminal investigations and intelligence, which allow to filter out passengers which corresponds to certain abstract profiles […]"[31]. According to the Commission, pre-determined criteria serve to "identify persons involved in criminal or terrorist activities who are, as of yet, not known to the law enforcement authorities.".[32]

First, the judgment restricted the "use of artificial intelligence technology in self-learning systems ('machine learning')", by prohibiting systems that are "capable of modifying without human intervention or review the assessment process and, in particular, the assessment criteria on which the result of the application of that process is based as well as the weighting of those criteria" (para 194). As previously noted[33], the exact scope of that prohibition is debatable. What is clear, however, is that the Court insists on the necessity of meaningful human intervention in predictive policing systems – a general principle already enshrined in Art. 11 of the Law Enforcement Directive. Central for its assessments was the "opacity which characterises the way in which artificial intelligence technology works" (para. 195), which may "deprive the data subjects […] of their right to an effective judicial remedy" (para 195).

The Court further highlighted the risk of discrimination. While the PNR Directive already acknowledged such risks in its Art. 6(4), the Court now also emphasised that that provision covers both direct and indirect discrimination (para 197). This is crucial because pre-established criteria may be based on seemingly innocuous personal data, which may, however, be proxies of prohibited characteristics. For example, a person's address may also be used as a

[31] Commission Staff Working Document SWD (2020) 128 final, 27 July 2020, page 11 footnote 36, accessible via: https://home-affairs.ec.europa.eu/system/files/2020-07/20200724_swd-2020-128_en.pdf, last accessed: 26 June 2023.

[32] Commission Staff Working Document SWD (2020) 128 final, 27 July 2020, page 24, accessible via: https://home-affairs.ec.europa.eu/system/files/2020-07/20200724_swd-2020-128_en.pdf, last accessed: 26 June 2023.

[33] Thönnes, A Directive altered beyond recognition, Verfassungsblog, 23 June 2022, https://verfassungsblog.de/pnr-recognition/, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

proxy for religion, race or ethnic origin. Algorithms must be “targeted, proportionate and specific” (para 198) and thus non-discriminatory – a finding with wider implications in the context of migration, where non-discrimination must be (but is not) embedded in the discretionary decision-making process. Used technologies will also have to comply with a set of additional quality standards: They will have to incorporate “incriminating” as well as “exonerating’ circumstances” (para 200), thus bolstering their reliability and reducing false-positive rates. The Court stated that high false-positive rates, which are present in Member States’ statistics[34], may undermine a system’s suitability and proportionality (see para 123). Thus, the CJEU stressed the necessity of regular reviews of the pre-determined criteria’s strict necessity (para 201). In addition, the Court underscored that the Data Protection Officer and national supervisory authorities must be equipped with robust rights of access to the content of pre-determined criteria (para 212).

Whilst acknowledging “the fairly substantial number of ‘false positives’”, the CJEU stressed that “the appropriateness of the system […] essentially depends on the proper functioning of the subsequent verification of the results […] by non-automated means” (para 124). For that purpose, the Court determined that Member States must “lay down clear and precise rules capable of providing guidance” for the review (para 205), which is meant to prevent both discriminatory results, and false matches to be transferred to the competent authorities, thus subjecting passengers to false suspicions of being involved in terrorist offences or serious crimes. It also aimed at reliable documentation and self-monitoring (para 207), as well as guaranteeing uniform administrative practices across PIUs in different Member States that observes the principle of non-discrimination. The results of individual human reviews must take preference over those of automated processing (para 208).

Finally, the judgment bolstered the right to an effective judicial remedy, as enshrined in Art. 47 of the Charter of Fundamental Rights of the European Union: “The competent authorities must ensure that the person concerned […] is able to understand how those criteria and those programs work”, so that they can “decide with full knowledge of the relevant facts whether or not to exercise [their] right to the judicial redress”, pursuant to Art. 13 of the PNR Directive (para 210). This seems to imply notification requirements in cases of verified positive matches

[34] Thönnes, On Flights, Rock Concerts and the Needle in a Haystack, EU Law Analysis, 17 September 2021, https://eulawanalysis.blogspot.com/2021/09/on-flights-rock-concerts-and-needle-in.html, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

which currently neither the PNR Directive nor most national transposition laws expressly contain.

Room for elaboration

Whereas the Court established an abundance of procedural safeguards to reign in the potential excesses of automated predictive threat detection, *Ligue des droits humains* also left a lot of open questions.

First, while the Court rightly flagged false-positives as a potential hurdle to a system's proportionality, it did not clarify at what point a system just produces too many of them, thus rendering the system disproportionate. Although this point was raised in the oral hearing[35], the Court also never addressed the base rate fallacy[36] undergirding the PNR system. The PNR Directive seeks to identify a very small number of potential terrorists and serious offenders within the general population of hundreds of millions of annual flight passengers. It therefore, like some other predictive policing systems, compels security authorities to look for the proverbial needle in the haystack. This can result in systemic flaws which make extremely high false positive rates a mathematical near-certainty. It remains to be seen whether mere procedural safeguards can succeed in saving the PNR system's suitability as long as its underlying base rate fallacy remains unaddressed.

Second, it remains unclear what purpose and form human interventions in the PNR system have to take, in particular, how humans are supposed to meaningfully engage with the PNR system's automated outputs. The Court delegated the formulation of "clear and precise rules" for human review to Member States (para 205) without providing them with much guidance. That PIU officials will be capable of meaningfully engaging with the PNR system's automated outputs seems doubtful when, for the foreseeable future, they will be confronted with thousands of false matches.

Third, whereas the Court's insistence on substantive human review is extremely important to prevent automation bias (an often-observed over-reliance on automatically generated

[35] See the report from the oral hearing in Thönnes, On Flights, Rock Concerts and the Needle in a Haystack, EU Law Analysis, 17 September 2021, https://eulawanalysis.blogspot.com/2021/09/on-flights-rock-concerts-and-needle-in.html, last accessed: 26 June 2023.

[36] See Epicenter.works, Why EU passenger surveillance fails its purpose, 25 September 2019, https://edri.org/our-work/why-eu-passenger-surveillance-fails-its-purpose/, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

recommendations)[37], there also remain questions regarding how human review is supposed to prevent direct and indirect discrimination, hamstrung by a phenomenon known as "selective adherence bias": Recent studies suggest that the 'human in the loop' may be predisposed to agree with those results of the automated processing that are more aligned with their personal pre-existing biases[38]. Such biases may be based on socially induced stereotypes, beliefs and social identities, and result in selective adoption of algorithmic advice. It is known that humans tend to be susceptible to confirmation bias, meaning that they assign greater weight to information congruent with prior beliefs and less to content that contradicts them. Whereas automation bias may be more easily detected, it may be more difficult to detect and prevent selective adherence bias, especially in cases where the competent authorities share the same (e.g. regional) biases as the PIU. This holds true especially when PIUs and competent security authorities receive an excess of potentially false matches. In practice, this could result in high risks of false suspicion for members of negatively stereotyped minority groups.

A decision to be remembered: Implications for ETIAS and CSAM

These gripes notwithstanding, the ruling does provide important guidelines on assessing other security-related instruments. Some of the aforementioned standards may be tailored to the PNR context. However, they pertain to features and risks that the PNR system shares with other security instruments aimed at preventively detecting threats in large datapools through automated processing. *Ligue des droits humains* is a decision to be remembered.

It will most likely be referred to if and when the CJEU is asked to assess two other recently introduced or proposed security instruments: The European Travel Information and Authorisation System (ETIAS) Regulation and the EU Commission's proposal for a Regulation on combating online child sexual abuse material (CSAM).

At first sight, ETIAS and the CSAM proposal may appear unrelated: What, after all, does the processing of visa-exempt third-country-nationals' applications for EU travel authorisations have to do with combating child sexual abuse material? The answer is that both legal instruments entail the use of the same tool for both purposes – potentially self-learning algorithms. In that regard, both instruments are spiritual successors to the PNR Directive (the

[37] See Lyell/Coiera, Automation bias and verification complexity: a systematic review, (2017) 24 Journal oft he Americal Medical Informatics Association, 423.

[38] Alon-Barkat/Busuioc, Human-AI Interactions in Public Sector Decision-Making: „Automation Bias" and „Selective Adherence" to Algorithmic Advice, (2023) 33 Journal of Public Administration and Theory, 153.

Electronic copy available at: https://ssrn.com/abstract=4547775

subject of *Ligue des droits humains*). Both undertake to automatically identify previously unknown material or persons in large datapools in order to protect public security – artificial intelligence, to the EU Commission, seems like a natural fit for that task.[39]

However, having public authorities – or even private entities, as is the case for the CSAM proposal – unleash such technologies for security purposes is confronted with significant rule-of-law concerns. The CJEU highlighted these concerns in *Ligue des droits humains*. We conclude that the judgment highlights certain rule of law shortcomings of ETIAS and raises concerns regarding the proportionality of the CSAM proposal.

The implications of Ligue des Droits Humains entails for ETIAS

The ETIAS Regulation requires visa-exempt third-country nationals to undergo pre-vetting through automated processing of the personal data they provide in their online application to obtain a travel authorisation to travel to the Schengen area.[40] Applicants' personal data will be processed, among others, against so-called "screening rules". These screening rules, according to Art. 33 (1) of the ETIAS Regulation, are "an algorithm enabling profiling […] through the comparison […] with specific risk indicators established by the ETIAS Central Unit […] pointing to security, illegal immigration or high epidemic risks." Frontex, where the ETIAS Central Unit is situated, is in charge of deploying algorithms for the purpose of detecting whether applicants pose any of the aforementioned threats. It is doubtful whether ETIAS is compatible with the standards the Court established for automated predictive threat detection in *Ligue des droits humains*.

To begin, it is unclear whether ETIAS complies with the Court's standards regarding "clear and precise" criteria ensuring meaningful human review. The Regulation itself does not contain such criteria, only stating that the ETIAS Central Unit should conduct an initial verification of any hit(s) (Art. 22 (3)). Hereupon, the ETIAS Central Unit forwards verified hits to the

[39] European Parliamentary Research Service, Dumbrava, Artificial intelligence at EU borders, July 2021, https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf, last accessed: 26 June 2023.

[40] For a more detailed description of ETIAS see Vavoula, Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism, (2021) 23 European Journal of Migration, 457; Guild/Vavoula, Travel authorization in the EU: automated processing and profiling, openDemocracy, 12 October 2020, https://www.opendemocracy.net/en/can-europe-make-it/travel-authorization-eu-automated-processing-and-profiling/, last accessed: 26 June 2023; Zandstra/Brouwer, Fundamental Rights at the Digital Border, Verfassungsblog, 24 June 2022, https://verfassungsblog.de/digital-border/, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

responsible ETIAS National Unit, which should then "assess" the risks in question (see Article 26 (3) lit. b, (4), (5), (6)). This wording is not "clear and precise" at all. It is questionable whether the specification of these standards can be delegated to Member States to the same extent as in the case of the PNR system. The latter is regulated by a Directive and therefore geared towards wide margins of discretion for Member States, while ETIAS was established by a Regulation.

Furthermore, having the EU legislature define the purpose and form of human intervention in decisions about ETIAS applications in a proper and transparent process is a matter of democratic legitimacy. While Member States' executives can certainly regulate the details, defining the purpose of human judgment and preventing its displacement by algorithms is not a technocratic sideshow. Therefore, the EU entities which enjoy the most democratic legitimacy should be meaningfully involved – not just the executive. This was also the issue when the Administrative Court of Wiesbaden decided that the German legislature must reform the German law transposing the PNR Directive (the Fluggastdatengesetz[41]), rather than completely delegating the implementation of *Ligue des droits humains* to the German PIU.[42] From an institutional perspective, without clear guidelines, ETIAS National Units may also not be in a position to ensure meaningful human intervention: Given that the screening rules are manufactured under the responsibility of Frontex (Art. 33 (4)), National Units may not have the necessary expertise on the inner workings of the ETIAS screening rules. While National Units will be supported by the ETIAS Screening Board and a "Practical Handbook", the former includes no independent supervisory entity (see Article 9 (2)), and the content of the latter remains underspecified in the Regulation (Art. 93). Leaving National Units completely in charge without clear guidelines and independent oversight may not only lead to false suspicion, but could also perpetuate discrimination through selective adherence bias: National Units may have their own, culturally- and historically-grown biases against certain groups of ETIAS applicants, thus creating an additional layer of direct and indirect discrimination.

One possible solution would be to strengthen the role of the ETIAS Central Unit beyond the formalistic manual verification of hits. This would require equipping the Central Unit, first,

[41] Acessible via: https://www.gesetze-im-internet.de/flugdag/BJNR148410017.html, last accessed: 26 June 2023.

[42] For the press statement issued by the *Verwaltungsgericht Wiesbaden* see here: https://verwaltungsgerichtsbarkeit.hessen.de/presse/verarbeitung-von-fluggastdaten-rechtswidrig, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

with clear and precise substantive criteria for determining potential risks and, second, with guidelines on how to prevent automation bias as well as selective adherence. Stakeholders with expertise in human rights at Frontex could be involved in the process and have the power to meaningfully influence the review process for compliance with human rights standards. For that purpose, the role and access rights of the ETIAS Fundamental Rights Guidance Board (see Art. 10) should be strengthened. Such an upgrade of the Central Unit's role could improve uniformity of administrative practices and compliance with the principle of non-discrimination. Of course, considering what is known about the agency's involvement in systematic human rights violations[43], there are concerns regarding the desirability of entrusting Frontex with additional tasks. Thus, any additional tasks delegated to the Agency must come tied to strong safeguards and robust oversight powers for the European Data Protection Supervisor.

Furthermore, ETIAS suffers from the opacity against which *Ligue des droits humains* cautions. The ETIAS screening rules have been criticised (here and here) for their lack of transparency.[44] The relevant delegated and implementing decisions of 23 November 2021[45] do virtually nothing to increase legal certainty either. Applicants' right to an effective judicial remedy is further undermined by the fact that notifications about negative decisions will not enable failed applicants "to understand how those criteria and those programs work" (*Ligue des droits humain*s, para 210). Art. 38 (2) (c) of the ETIAS Regulation only provides for the communication of the category of data processed, rather than a human-centered communication of the grounds of refusal.[46] The mandatory form used for refusals of travel, as prescribed by the Commission implementing decision 2022/102[47], does not instruct administrators officers on how to meaningfully substantiate their assessment with relevant facts. Though the form contains a free text field, the implementing decision does not contain

[43] See Human Rights Watch, Frontex Failing to Protect People at EU Borders, 23 June 2021, https://www.hrw.org/news/2021/06/23/frontex-failing-protect-people-eu-borders, last accessed: 26 June 2023.

[44] Vavoula, Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism, (2021) 23 European Journal of Migration, 457; Derave/Genicot/Hetmanska, The Risks of Trustworthy Artificial Intelligence: The Case of the European Travel Information and Authorisation System, (2022) 13 European Journal of Risk Regulation, 389.

[45] Commission Delegated Decision of 23 November 2011 on further defining security, illegal immigration or high epidemic risks, C(2021) 4981 final, accessible via: https://ec.europa.eu/transparency/documents-register/api/files/C(2021)4981_0/090166e5e91548a4?rendition=false, last accessed: 26 June 2023; Commission Implementing Decision of 23 November 2021 on specifying risks related to security, illegal immigration or high epidemic risks as defined in Regulation (EU) 2018/1240 of the European Parliament and of the Council.

[46] See also Zandstra/Brouwer, Fundamental Rights at the Digital Border, Verfassungsblog, 24 June 2022, https://verfassungsblog.de/digital-border/, last accessed: 26 June 2023.

[47] Commission Implementing Decision (EU) 2022/102 of 25 January 2022 laying down forms for refusal, annulment or revocation of a travel authorisation, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.017.01.0059.01.ENG, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

requirements on how comprehensive the text accompanying the refusal of a travel authorisation should be.

Proposed CSAM Regulation clashes with Ligue des Droits Humains

The findings in *Ligue des droits humains* may be relevant for the Commission's proposal for a Regulation laying down rules to prevent and combat child sexual abuse (CSAM proposal). The proposal constitutes a prime example of privatised surveillance, similar to the PNR Directive, whereby private companies or professions are called on to cooperate with state authorities in the fight against crime. It also forms part of an emerging legal framework on online content moderation, comprising the Digital Services Act[48] and Regulation (EU) 2021/784[49] on addressing the dissemination of terrorist content online. However, the proposed rules go beyond the other legal instruments. In order to combat sexualised violence against children, the proposed Regulation, among other things, authorises competent national courts or independent administrative authorities, upon request by designated national "Coordinating Authorities", to issue "detection orders" (Art. 7 (1)). Such detection orders, as per Art. 10 (1), oblige providers of hosting services, such as Facebook or Youtube, or interpersonal communication services, such as Whatsapp, to use automated systems to detect and report not only known, but also new child sexual abuse material and grooming. While known and classified CSAM can be recognised through an image's digital quasi-fingerprint (so-called hashes), this is not possible for unknown CSAM. Automatically detecting the latter is only possible by first training self-learning algorithms based on pattern recognition in previously classified CSAM material (see for that purposes Arts. 44 and 36) and then unleashing them on all users of the service in question. Thus, with regard to unknown CSAM and grooming, the CSAM rules entail generalised reporting obligations and genenalised surveillance of all users' interpersonal communications. As a result, the CSAM proposal has been criticised for violating Articles 7 and 8 of the Charter.[50] In addition to this critique, the CSAM proposal is not in line

[48] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), accessible via: https://eur-lex.europa.eu/eli/reg/2022/2065/oj, last accessed: 26 June 2023;

[49] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32021R0784, last accessed: 26 June 2023.

[50] Bäcker/Buermeyer, My spy is always with me, Verfassungsblog, 18 August 2022, https://verfassungsblog.de/my-spy-is-always-with-me/, last accessed: 26 June 2023; Legal Opinion by Ninon Colneric, accessible via: https://www.patrick-breyer.de/wp-content/uploads/2021/03/Legal-Opinion-Screening-for-child-pornography-2021-03-04_incl_Logos.pdf, last accessed: 26 June 2023; European Parliamentary Research Service, Draft Impact Assessment on the Proposal for a regulation laying down the rules to prevent

Electronic copy available at: https://ssrn.com/abstract=4547775

with the CJEU’s standards for automated predictive threat detection, as established in *Ligue des droits humains*.

First, the CSAM proposal does not comply with the standards established in *Ligue des droits humains* regarding transparency and legal contestability. When screening their users’ communication, it is unclear how it can be guaranteed that private service providers will comply with established rule of law standards. The proposal allows but does not require them to use the screening software developed by the EU Centre on Child Sexual Abuse software (see Art. 10 (2)), thus opening the door for non-transparent, commercial software. It is not clear how supervisory authorities, such as the EDPS, can guarantee that the software in use is compliant with non-discrimination and other quality standards. The CSAM proposal does not provide access to source codes for supervisory authorities or affected persons. In fact, it deliberately curtails access to databases of indicators in the name of security (Art. 46). Given the additional lack of stringent notification and explanation requirements, CSAM algorithms are likely to produce high amounts of false and stigmatising suspicion, based on opaque and hard-to-challenge rules – precisely the sort of thing the *Ligue des droits humains* standards seek to prevent.

Moreover, the CSAM proposal raises concerns regarding the Court’s pronouncements on high false positive rates. The Court links the severity of interferences with fundamental rights to the reliability of the AI technology used – the higher a system’s false positive rate, the higher its interference with fundamental rights. Distinguishing CSAM from legal content (such as consensual sexual activity among teenagers, medical or family photos) is highly context-dependent, with regards to both the content as well as the modes of production and dissemination. In the foreseeable future, no AI system will be capable of such a complex contextual assessment. Additionally, the CSAM proposal would perpetuate the PNR system’s base rate fallacy problem. Rather than deploying algorithmic profiling in a targeted way (for example, within databases of known prior offenders, or empirically proven CSAM-prone places, such as certain dark net forums), designated service providers will have to sift through

and combat child sexual abuse, accessible via: https://cdn.netzpolitik.org/wp-upload/2023/04/2023-04-05_EPRS_CSAM_Complementary-Impact-Assessment_DRAFT.pdf, last accessed: 26 June, 2023; see also the expert statements from the German Bundestag, accesible via: https://www.bundestag.de/ausschuesse/a23_digitales/Anhoerungen/932296-932296, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

all their online communication to find CSAM 'needles in a haystack' consisting of billions of private messages on short notice.

According to *Ligue des droits humains*, systems with a "fairly substantial number of false positives", "depend on the proper functioning of the subsequent verification of the results […] by non-automated means" (para 124), in order to guarantee their proportionality. This review must be guided by "clear and precise rules" (para. 205). The CSAM proposal, however, just like ETIAS, contains no precise rules for that purpose, only stipulating that the EU Centre on Child Sexual Abuse – an agency specifically created for the Regulation's implementation – should throw out "manifestly unfounded" reports (Art. 48 (2)), and stating that the training data must be chosen in a "diligent assessment" per Art. 36 (1). Moreover, the extremely intimate nature of the communication contents in question and the review process itself – irrespective of its result – already constitutes a particularly serious interference with Articles 7 and 8 of the Charter and arguably a violation of the essence of these rights. After all, complete strangers will, without users' consent or knowledge, view their intimate private messages which may often describe sexualised activity or depict nudity.

Another aspect in which the CSAM proposal raises concerns similar to issues touched upon by the judgment is that it indiscriminately interferes with the exercise of a fundamental freedom within the EU. While being quite lenient when it comes to extra-EU flights, due to traditional border controls at the EU's external borders, *Ligue des droits humains* insists on much stricter selection standards when it comes to using travel within the EU as an occasion for mass data retention and processing. In paragraphs 279 and onwards, the Court emphasised that mass data retention and processing regimes undermine the freedom of movement[51] and the absence of internal border controls[52], unless there is "a genuine and present or foreseeable terrorist threat" (para. 291). This rationale can be extended to the CSAM proposal *a fortiori*: Whereas being subjected to scrutiny when travelling is expected to some extent, the same cannot be said for private communications. Confidentiality of communications forms part of the right to privacy and is a reasonable expectation within EU Member States. The CSAM detection orders shatter this expectation, thus curtailing and creating chilling effects for the free flow of communication and the freedom to conduct a business, enshrined in Art. 16 of the Charter. Users and providers

[51] Art. 45 of the Charter, Art. 20 (2) (b) TFEU.

[52] Art. 67 (2) TFEU.

Electronic copy available at: https://ssrn.com/abstract=4547775

of the targeted services could be deterred from engaging in legal (and even desired) activities because they fear sanctions.

According to *Ligue des droits humains*, this risk must be limited through specific selection criteria to guarantee that the freedoms at play may only be curtailed as a proportionate response to a specific threat. In the context of air travel, the Court required limitations to "certain routes or travel patterns or to certain airports, stations or seaports" (para. 291). Art. 7 (4) (a) of the CSAM proposal does stipulate that judicial authorities may only permit a detection order when there is "evidence of a significant risk of the service being used for the purpose of online child sexual abuse". Section 6 provides that for detection orders regarding new CSAM, previous mitigation measures, as well as detection orders regarding known CSAM, must have been unsuccessful. These selection criteria, however, do not rise to the level of specificity required by the Court. A detection order could still pertain indiscriminately to all communication transmitted by a service provider, so potentially billions of messages. The movement-based equivalent of such detection orders would be to oblige a market-dominating airline or bus company to transmit data about all their travel connections for automated predictive threat detection. The Court's criteria, however, are location-based. A reasonable equivalent for "airports, stations or seaports", irrespective of their technical feasibility, would be detection orders pertaining to specified CSAM-prone communication nodes, like URLs, dark net forums, servers or chat groups. The detection orders, as established in the CSAM proposal, would therefore indiscriminately curtail the free flow of communication and services within the EU and would therefore be disproportionate according to the logic of *Ligue des droits humains*.

Conclusion

This contribution aimed to bring together the PNR decision's consequences for other security-related instruments engaging in automated predictive threat detection. In the case of ETIAS, though an immigration control tool, one of its explicitly stated purposes is to contribute to a high level of security (Art.4 (1) (a)), thus, as in the case of the PNR Directive, it hovers in-between an immigration and security tool encompassing surveillance of mobility. As for CSAM, much as the PNR Directive, it exemplifies privatised surveillance, but in this case the predictive threat detection itself is delegated to the private sector without sufficient safeguards. We argued that, in pursuing similar strategies, both the ETIAS Regulation and the CSAM proposal are not in line with *Ligue des droits humains* in very similar ways. Shedding light into

Electronic copy available at: https://ssrn.com/abstract=4547775

both systems' shortcomings has demonstrated that the decision will be crucial for the future development of EU security law. Further forward-looking, innovative scholarship is needed to gain a solid grasp of the implications of this complex and challenging decision.

Electronic copy available at: https://ssrn.com/abstract=4547775

Machine learning and profiling in the PNR system

Janneke Gerards

The Passenger Name Record (PNR) Directive[53], adopted in 2016, has led to significant debate among lawyers. Several preliminary references have been made to enquire into its interpretation and validity. In 2022, one of these led to the landmark judgment of the CJEU in *Ligue des droits humains*[54]. As this series of blogposts on the PNR judgment show, this is a rich judgment with many very interesting elements, among which are the CJEU's considerations related to non-discrimination. Indeed, automated processing of personal data, which is what PNR data are, can lead to forms of profiling, in the sense that certain individuals or groups of people are more likely to be excluded based on the transfer of their data than others. If those people are also found to have certain characteristics, such as a particular ethnic or national origin or religion, they may be directly or indirectly disadvantaged, in violation of the prohibition of discrimination. In its judgment, the CJEU extensively discusses these discrimination risks, and it set a number of conditions to prevent them. Unfortunately, as the present post aims to further explain, not all of its considerations are perfectly clear and some of the solutions the CJEU proposes are not entirely satisfactory.

Safeguards against discrimination in the PNR Directive

As such, the PNR Directive contains several safeguards against discrimination. According to Article 6(2) of the PNR Directive, a Passenger Information Unit (PIU; the national police units in charge of receiving, processing, and further sharing of the passenger data), may only process PNR data for a limited number of purposes. Most relevant when it comes to non-discrimination is the (a) ground. This relates to the assessment whether certain passengers should be subject to further examination because they might be involved in a terrorist offence or serious crime. For the purpose of that assessment, the competent PIU may firstly compare the PNR data with, for example, databases containing information related to wanted or reported persons (Art. 6(3)(a) of the PNR Directive). If that information leads to a match, the PIU may transmit the data to the competent authorities of a Member State, which may take action on that basis. In addition, Article 6(3)(b) allows a PIU to process PNR data "against pre-determined criteria".

[53] Directive (EU) 2016/681, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0681, last accessed: 26 June 2023.
[54] CJEU, Case C-817/19 *Ligue des droits humains* [21 June 2022].

Electronic copy available at: https://ssrn.com/abstract=4547775

The assessment of the data according to these criteria must, according to paragraph 4, be carried out “in a non-discriminatory manner”. Also, according to this paragraph, the predetermined criteria must be “targeted, proportionate and specific”. They must be regularly reviewed and shall ‘in no circumstances be based on a person’s race, ethnic origin, religious, philosophical or political beliefs, trade union membership, health, sex life or sexual orientation”. Insofar as relevant, Article 6(5) additionally stipulates that automatic processing operations to see whether certain passengers may be subject to further scrutiny should be checked on a case-by-case basis in a non-automated manner – that is, manually, by humans.

‘Pre-determined criteria’ and machine learning algorithms

As Advocate General Pitruzella[55] has explained, setting such pre-determined criteria involves profiling: certain criteria are used to ‘predict’ which passengers might be involved in a terrorist crime or serious crime (para. 223). In a first evaluation[56] of the PNR Directive, the European Commission gave the following definition of pre-determined criteria: “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 correspond 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.” Accordingly, profiles are made based on individual characteristics, which, taken together, may reveal a risk for certain behaviour in the future. Unfortunately, however, the Directive does not explain how and on what grounds these targeting rules can be established, what data may be used to do so, or where that data may be sourced from.

In *Ligue des droits humains*, the CJEU concentrated on the use of these pre-determined criteria. In particular, it ruled that the requirement that criteria must be ‘pre-determined’ “[…] precludes the use of artificial intelligence technology in self-learning systems (‘machine learning’), capable of modifying without human intervention or review the assessment process […]” (para. 194). This consideration of the CJEU is rather ambiguous[57], but it seems to imply that the use of machine learning algorithms (hereafter: ‘ML algorithms’) to set pre-determined criteria can only be accepted if very strict conditions are met. However, to understand the importance of

[55] Opinion of Advocate General Pitruzzella, C-817/19 *Ligue des droits humains* [27 January 2022].
[56] https://home-affairs.ec.europa.eu/system/files/2020-07/20200724_swd-2020-128_en.pdf, last accessed: 26 June 2023.
[57] Thönnes, A Directive altered beyond recognition, Verfassungsblog, 23 June 2023, https://verfassungsblog.de/pnr-recognition/, last accessed: 26 June 2023

Electronic copy available at: https://ssrn.com/abstract=4547775

the PNR judgment for the use of ML algorithms, and to be able to deal with its ambiguity, it may be good to first briefly explain how such algorithms work. To put it very simply, an algorithm can be 'taught' to detect strong similarities and correlations in large datasets and to determine statistical relationships and probabilities – for instance, the probability that someone who is showing certain characteristics and behaviour is preparing a terrorist attack. This teaching and learning is done through a feedback system. For example, a programmer will give the algorithm positive feedback if it has correctly detected a person as setting a particular risk, as that person has been convicted of terrorism in the past. Conversely, the programmer will give negative feedback if the algorithm has wrongly identified someone as likely to be involved in terrorism. In this way, the algorithm's pattern recognition is constantly being refined and improved. The more often this feedback process is repeated, the more accurately the algorithm's predictions will become, until a point that it can be validated and be used in practice.

During the training process, the algorithm may be taught not to take into account any of the characteristics[58] listed in Article 6(4). A well-trained algorithm is then unlikely[59] to readily identify factors such as 'origin of country x' or 'member of religious group y' as criteria relevant to determining whether a passenger is likely to have terrorist or criminal intentions. Instead, the algorithm will look for other patterns in the plethora of information that may be available about people who have committed serious criminal offences or terrorism in the past. In doing so, an algorithm does not use the same causality-oriented logic as humans.[60] Instead, an algorithm looks for statistically significant relationships (correlations) between certain factors. As a result, an algorithm may find, for example, that within a dataset there is a correlation between terrorist behaviour and seemingly illogically related factors such as late booking, searching the internet for information about planes, frequenting the toilet at the airport and sending messages in a certain language. Perhaps human beings might not easily think of the combination of such factors as relevant or causally related to terrorism. However, because

[58] Kamiran/Calders/Pechenizkiy in: Custers/Calders/Schermer/Zarsky (eds), Discrimination and Privacy in the Information Society (Springer 2013), 223.

[59] Žliobaitė/Custers, Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models, (2016) 24 Artificial Intelligence and Law, 183.

[60] Information Society (Springer 2013), 223.

[60] Žliobaitė/Custers, Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models, (2016) 24 Artificial Intelligence and Law, 183.

[60] Žliobaitė/Custers, Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models, (2016) 24 Artificial Intelligence and Law, 183.

Electronic copy available at: https://ssrn.com/abstract=4547775

it might be correlated to a risk of terrorism or serious crime, it still could provide a pre-determined criterion[61] to start processing PNR data.

To many people, the method discussed above may seem very useful. However, the CJEU rightly identified a number of considerable drawbacks related to the deployment of ML algorithms and profiling, especially when viewed from the specific perspective of the prohibition of discrimination.

Discrimination-related problems of ML algorithms

A first problem is the so-called base rate fallacy[62]. This means that, however carefully an algorithm is trained, it may still identify 'false positives' or 'false negatives'. In other words, it can happen that the algorithm either wrongly designates a person as constituting a risk, or it misses a person who would present a risk. So that either means wrongly identifying someone as potentially suspicious, or overlooking an actual risk of terrorism or serious crime. Both are clearly problematic[63], but there is research pointing out that the PNR system causes an especially high risk of false positives.[64]

Another problem is that a machine learning algorithm can only operate properly when it is trained on a good dataset.[65] It must be relevant to the specific European context, it must contain enough data, it must be representative of the kind of information that is needed, and so on. It proves very difficult to compile or obtain those kinds of datasets and prevent them from reflecting discriminatory and stereotypical patterns in human thought and action.[66] The well-known risk of 'rubbish in is rubbish out'[67] then easily arises, in that deficiencies and discrimination in the data soon translate into inaccuracies and discrimination in the output of an algorithm. Moreover, if a dataset is not properly set up and prepared, it can severely disrupt

[61] Orrù, The European PNR Directive as an instance of pre-emptive, risk-based algorithmic security and its implications for the regulatory framework, (2002) 27 Information Polity, 131.

[62] Borgesius, Strengthening legal protection against discrimination by algorithms and artificial intelligence, (2020) 24 The International Journal of Human Rights, 1572.

[63] Korff, Passenger Name Records, data mining & data protection: the need for strong safeguards, Council of Europe T-PD (2015)11, 15 June 2015, https://rm.coe.int/16806a601b, last accessed: 26 June 2023.

[64] Thönnes, A cautious green light for technology-driven mass surveillance, Verfassungsblog, 28 January 2022, https://verfassungsblog.de/green-light/, last accessed: 26 June 2023.

[65] Information Commissioner's Office, Big data, artificial intelligence, machine learning and data protection, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf, last accessed: 26 June 2023.

[66] Hacker, Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law, (2018) 55 Common Market Law Review, 1143.

[6767] Barocas, Selbst, Big Data's Disparate Impact, (2016) 104 California Law Review, 671.

Electronic copy available at: https://ssrn.com/abstract=4547775

the learning process. For instance, an algorithm may learn to recognise certain patterns as relevant on the basis of non-representative or incorrect data, when in reality those patterns turn out to be incorrect. In that case, the risk of false negatives and false positives increases even more. This risk is amplified if the algorithm continues to 'improve' itself in practice by recognising patterns independently in newly added (also coloured) data. This can lead to reinforcement of already existing forms of (institutional) discrimination.[68] For PNR algorithms, the lack of good datasets is a well-known problem. The European Parliament's research office has pointed out[69] that data obtained from airlines or under PNR agreements with third countries are very unreliable. As a result, there is a high risk of discrimination through the use of ML algorithms.

Third, the Court has observed that training an algorithm is similar to taking a snapshot. At a certain point in the training process, an algorithm is validated and found suitable to perform. But then, in practice, the datasets the algorithm works with are constantly changing. Information may continuously be added about suspected and convicted or acquitted people, or about their behaviour and habits. An algorithm that cannot adapt to such new data would quickly lose its relevance. Therefore, many ML algorithms are self-learning and can continue to update themselves[70] by looking for useful correlations even in new data. That keeps the algorithm up-to-date, but it also makes it very easy to lose grip on how it works.

Finally, as noted above, risk assessments must not take account of protected personal characteristics, such as gender or ethnic origin. However, because an algorithm looks for correlations in a very fine-grained manner, it is difficult to fully prevent discrimination on these grounds. ML algorithms are easily able to establish correlations between seemingly harmless factors, such as times when someone is on their phone, distance from one's home to the airport or a preference for travelling by bus. Yet, in practice, even these factors can sometimes provide clues about someone's ethnicity, religious or political affiliation and may result in 'proxy

[68] European Commission, Directorate-General for Justice and Consumers, Gerards, Xenidis, Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination in Europe, 2021, https://op.europa.eu/en/publication-detail/-/publication/082f1dbc-821d-11eb-9ac9-01aa75ed71a1, last accessed: 26 June 2023.

[69] European Parliamentary Research Service, Dumbrava, Artificial intelligence at EU borders, July 2021, https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf, last accessed: 26 June 2023.

[70] European Commission, Directorate-General for Justice and Consumers, Gerards, Xenidis, Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination in Europe, 2021, https://op.europa.eu/en/publication-detail/-/publication/082f1dbc-821d-11eb-9ac9-01aa75ed71a1, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

discrimination'[71]. It is difficult to eliminate this without making an algorithm completely ineffective. Moreover, it is far from easy to find out whether there is proxy discrimination, because it is usually not very clear exactly which constellations of factors an algorithm detects as a relevant pattern. Indeed, this is what the CJEU held against algorithmic profiling: "given the opacity which characterises the way in which artificial intelligence technology works, it might be impossible to understand the reason why a given program arrived at a positive match" (para. 195).

The CJEU's response

These problems explain why the CJEU has set such strict conditions for the use of ML algorithms in risk profiling in its judgment in the PNR case. Rather than having an algorithm do the work, the Court seems to prefer the pre-determined criteria either to be set or at least to be applied or checked by human beings, for example, by officials working at the PIUs. According to the Court, in processing the data, the PIU and the competent authorities "can inter alia take into consideration specific features in the factual conduct of persons when preparing and engaging in air travel which, following the findings of and experience acquired by the competent authorities, might suggest that the persons acting in that way may be involved in terrorist offences or serious crime" (para. 199). In addition, the pre-determined criteria must meet several other requirements: they cannot be directly or indirectly discriminatory; they must meet the requirements of purposefulness, specificity and proportionality; they must take account of both incriminating and exonerating elements; and the number of false positives must be limited as much as possible.

It is unclear how discrimination can be prevented by these requirements, which could explain why the judgment can appear to be rather confusing. In fact, it seems that the Court's suggestions in paragraph 199 mean that the role of a predictive algorithm is effectively taken over by humans[72], who would come up with risk assessments based on their own experiences and actual observations, and would correct the algorithmic output and predictions accordingly. This 'human in the loop' approach might seem attractive, but human beings, too, are prone to

[71] European Commission, Directorate-General for Justice and Consumers, Gerards, Xenidis, Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination in Europe, 2021, https://op.europa.eu/en/publication-detail/-/publication/082f1dbc-821d-11eb-9ac9-01aa75ed71a1, last accessed: 26 June 2023.

[72] Orrù, The European PNR Directive as an instance of pre-emptive, risk-based algorithmic security and its implications for the regulatory framework, (2002) 27 Information Polity, 131.

Electronic copy available at: https://ssrn.com/abstract=4547775

stereotyped thinking. The kind of patterns they think they can observe can be very stigmatising. Consequently, one risk of discrimination is simply replaced by another one. Moreover, it is far from obvious that human profiling would lead to fewer false positives and negatives, or would be more transparent than a human prediction. Hence, the Court's strong emphasis on 'human intervention or review' certainly is not a sufficient guarantee against discrimination.

Fortunately, the Court added several considerations on the procedural safeguards that should accompany the use of pre-determined criteria. Their use should be based on a coherent administrative practice in which the principle of non-discrimination is paramount (para. 205). Checks of algorithmic output should be based on clear, precise and objective monitoring criteria that can help determine whether a person is indeed potentially involved in terrorism or serious crime (para. 206). There should be accurate documentation of the processing to enable verification and internal control of its lawfulness and stakeholders should be able to understand the criteria and the programmes that work with them (para. 207). This would enable them to avail themselves of legal protection options. If those options are used, the courts should be able to take note of all the relevant criteria and check how the programmes work (para. 210). The same applies to national supervisory authorities, who should be able to check that there was no discrimination (para. 212).

Indeed, such procedural safeguards are highly useful and offer better protection against the discriminatory use of ML algorithms than the Court's suggestions as to human intervention. It might have been even better if the CJEU had also ruled that machine learning algorithms may only be deployed if sound non-discrimination safeguards are built into the programming and training processes[73] and if mechanisms are put in place to detect and counteract discriminatory output. Nevertheless, to the extent the Court emphasises the need for multiple procedural safeguards when deploying algorithms, its ruling has considerable added value.

[73] European Commission, Directorate-General for Justice and Consumers, Gerards, Xenidis, Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination in Europe, 2021, https://op.europa.eu/en/publication-detail/-/publication/082f1dbc-821d-11eb-9ac9-01aa75ed71a1, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

Passenger Name Records and Security

Didier Bigo, Stefan Salomon

Security is not a transparent concept, but a contested one. There is no single form of security (national or global), but different forms of security (or in-security processes) that might be contradictory and mutually destructive. That is true for the notions of "preventive security" on the one hand, and of "policing security" on the other. The latter refers to targeted actions which respond to prognoses about concrete individual cases. Its legal framework is that of criminal law, based on a logic of inquiry, evidence-based investigation, and the presumption of innocence, even when it involves intelligence-led policing. In contrast, the new paradigm of preventive security relies on generalised surveillance and on a logic of general suspicion. Its principal legal field is that of administrative law and it operates through predictive tools that produce new 'realities'[74] by establishing correlations and patterns between seemingly unrelated facts. In this sense, preventive security is creative – not merely reactive. Preventive security and policing security are largely incompatible.

The EU Passenger Name Records (PNR) Directive[75] is based on the logic of preventive security. In this post, we describe the emergence of preventive security, how it entered into and eventually transformed PNR collection from a commercial activity into a security tool, and radically reshaped the work of border guards. Finally, we highlight the possible effects of the Court of Justice of the European Union (CJEU)'s PNR decision (*Ligue des droits humains*)[76] on the operation of preventive security measures. We argue that the judge of the CJEU did not simply accept a preventive security argument, and curbed its expansion, which may help security services to enhance their efficiency and legitimacy.

Inventing "preventive" security via "predictive tools"

Following the events of 9/11 in the US, the 9/11 Commission Report[77] and the administration under President George W. Bush considered that policing as security practice had become

[74] Just/Latzer, Governance by Algorithms: Reality Construction by Algorithmic Selection on the Internet, (2016) 39, Media, Culture & Society, 238.
[75] Directive (EU) 2016/681, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0681, last accessed: 26 June 2023.
[76] CJEU, Case C-817/19 *Ligue des droits humains* [21 June 2022].
[77] Accessible via: https://www.9-11commission.gov/report/911Report.pdf, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

obsolete in light of the peculiar threats that the US faced. The terminology of 'terrorist attacks', adopted by the US administration, shifted the terrorist acts by Al-Qaeda and Osama bin Laden from grave criminal acts into the register of war. This, in turn, triggers particular executive privileges, limited judicial review and an elevated role for intelligence services fighting an allegedly "stealth" enemy[78]. The covertness of the adversary and the US government's fear of a possible use of biological, chemical and nuclear weapons[79] resulted in policies that sought to anticipate terrorist acts before they happened. Donald Rumsfeld, then Secretary of Defence in the Bush administration, famously claimed that it was necessary to discover and anticipate unknown unknown threats[80] through Total Information Awareness (TIA). TIA, renamed later to Terrorism Information Awareness, was a mass surveillance program under the portfolio of the Department of Defence.

The objective of the TIA program was to collect and systematically correlate all electronic data on passengers landing on US territory through integrating different information technologies. The use of technologies capable of detecting 'weak signals' – the hidden network of relationships a data point has within vast amounts of data on the past and present behaviour of passengers – was seen as a revolutionary method to prevent terrorist offences. It was legitimised by the 1% doctrine[81]: if it was necessary to surveil and detain 99 innocent persons in order to identify one terrorist, the measures were considered justified.

In September 2003, the US Congress eventually defunded the TIA program[82] due to concerns about the mass collection of US citizens' personal data.[83] However, US intelligence services continued to use several of the TIA program's features. The US government considered internet and smartphone surveillance, along with tools to locate and identify passengers travelling to US territory, as the way forward to ensure national and global security in a context of transnational terrorism.

[78] Rotella, Al Qaeda's Stealth Weapons, Los Angeles Times, 20 September 2003, accessible via: https://www.latimes.com/archives/la-xpm-2003-sep-20-fg-converts20-story.html, last accessed: 26 June 2023.
[79] See former US President George W. Bush's speech „World Can Rise to This Moment" of 6 February 2003, accessible via: https://georgewbush-whitehouse.archives.gov/infocus/iraq/news/20030206-17.html, last accessed: 26 June 2023.
[80] See https://www.youtube.com/watch?v=REWeBzGuzCc, last accessed: 26 June 2023.
[81] See Suskind, The One Percent Doctrine (Simon & Schuster 2006).
[82] See Congressional Record of 24 September 2003, accessible via: https://sgp.fas.org/congress/2003/tia.html, last accessed: 26 June 2023.
[83] See Safire, You Are a Suspect, The New York Times, 14 November 2002, accessible via: https://www.nytimes.com/2002/11/14/opinion/you-are-a-suspect.html, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

The origins, expansion and complexification of PNR

The use of PNR data as a security tool was a result of the idea that it was necessary to "act before the next attack".[84] Congress adopted the US Aviation and Transportation Security Act[85] in order to monitor passengers and generalise electronic pre-border checks, despite concerns of airline carriers, foreign governments and the International Airline Transport Authority. Airlines which refused to transfer their commercial passenger data to US authorities would not be permitted to operate on US territory. In order to transfer passenger data, airlines were required to organise their information based on a PNR list of 34 security criteria (further reduced to 17 in 2016), which included relational and situational elements, such as the seat number, used to check whether nearby seats were occupied by a suspected person. The US Aviation and Transportation Security Act therefore transformed PNR data from a mere commercial activity by airline carriers into a security tool for US authorities.

The origins of PNR data use as a security tool are clear. However, global reactions differed. While some countries were averse to the idea that their national airline carriers would transfer PNR data to US authorities, others were enthusiastic. The EU, among others, concluded an agreement with the US on the transfer of advance passenger information and PNR data.[86] The UN Security Council, in the context of foreign nationals travelling to Syria to join the Islamic State, elevated the transfer of PNR data to a global "best practice" standard that all UN member states should adopt in their national laws (UNSC Resolution 2178 (2014), para 9-11[87] and UNSC Resolution 2396 (2017)[88]).

At the same time, concerns emerged about the protection of personal data, among others. In 2017, the CJEU held in Opinion 1/15 that the EU-Canada PNR agreement would be contrary to Articles 7 (respect for private and family life), 8 (right to protection of personal data), and

[84] Perry, Preparing for the Next Attack, Foreign Affairs, 1 November 2001, accessible via: https://www.foreignaffairs.com/articles/united-states/2001-11-01/preparing-next-attack, last accessed: 26 June 2023.

[85] Accessible via: https://www.congress.gov/bill/107th-congress/senate-bill/1447, last accessed: 26 June 2023.

[86] Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22012A0811%2801%29&qid=1682706316232, last accessed: 26 June 2023.

[87] Accessible via: https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F2178(2014)&Language=E&DeviceType=Desktop&LangRequested=False, last accessed: 26 June 2023.

[88] Accessible via: https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F2396(2017)&Language=E&DeviceType=Desktop&LangRequested=False, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

21 (right to non discrimination) of the Charter of Fundamental Rights of the European Union, among others, because the agreement neither prevented the transfer of sensitive personal data to Canada, nor discriminatory results of data processing.[89] In a similar vein, the Council of Europe's Consultative Committee of Convention 108 highlighted that PNR measures strongly interfered with the right to data protection under the European Convention of Human Rights. Although human rights, especially the right to protection of personal data, became a gateway to criticise the preventive security paradigm that undergirds PNR measures, the human rights critique did not directly address the principal issue concerning PNR data: the shift to generalised preventive security.[90]

Moreover, the complexification of PNR from its origins to the present day is a process in which multiple interests have reshaped the regulatory landscape. In this process, the EU has not simply followed US developments. The PNR Directive is born also from the EU's preoccupations with irregular migration. Already in the 1990s, years before the adoption of the PNR Directive, European police authorities integrated information on crime, terrorism, and irregular migration through the Schengen Information System (SIS)[91], thus maintaining access to different datasets for police and border guard authorities. The 2004 Madrid bombings then contributed to a considerable function creep. Police authorities increasingly gained access to databases used for other purposes than crime, especially databases on asylum and border crossings – a trend which was further reinforced by SIS 2 in 2013, which upgraded the SIS into a search engine.

The process of rendering databases interoperable was mainly driven by data engineers and intelligence services. Although anti-terrorist specialists at police authorities considered that internal threats would not be addressed by shifting the policy focus on external threats, they nevertheless considered it useful to add border control as an additional layer to already existing surveillance instruments. The narrative that democratic governments are active and closely cooperate to protect their population based on a strategy of prevention and prediction (the

[89] CJEU, Opinion 1/15 of the Court [26 July 2017], para 328.

[90] Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Opinion on the Data protection implications of the processing of Passenger Name Records, T-PD(2016)18rev, 19 August 2016, accessible via: https://rm.coe.int/16806b051e, last accessed: 26 June 2023.

[91] 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, available via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02018R1862-20220801, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

famous 3Ps[92]), provided public legitimacy to expanding instruments of intelligence services to areas of policing and immigration control. The upshot is that the legitimacy of the idea of preventive security remained unchecked, appearing as additional – and not contradictory – to the logic of security in policing.

Transformations of security professionals' practices

The expansion of surveillance instruments and the consolidation of preventive security in immigration controls over the last twenty years fundamentally changed the everyday work of border guards. Border guards, who are at the frontline of controlling travel documents, turned into a sort of secondary policemen. This created unease about the 'intelligencification' of their activities and uncertainties among border guards on what their role actually is.[93]

At the same time, the development of human and technological resources, which organise the interoperability of databases for collecting, storing, sorting, and sharing passengers' data, remained largely shielded from public attention. These developments involved not only public but also private actors with considerably greater resources to produce more accurate technology within a shorter span of time. Technological developments in the private sector occurred especially through the advance of proprietary software, often shrouded in secrecy, that use algorithms and machine-learning processes.[94] Algorithms and machine learning, in turn, facilitate the use of predictive tools that establish risk scores and assign personalised risk factors to suspects on watch lists.

The result of these developments was the normalisation of surveillance technologies developed by the private sector beyond their commercial use. These technologies' margins of error remain significant: more than four out of five individuals flagged by PNR measures are false positives, and thus subjected to false suspicion.[95] From the perspective of security studies, the expansion

[92] Bigo, International flows, political order and social change: (in)security, by-product of the will of order over change, (2017) 18 Global Crime, 303.
[93] Andersson, Illegality, Inc. (University of California Press 2014).
[94] van Brakel in Schuilenburg/Peeters (eds), The Algorithmic Society (Routledge 2020), 99.
[95] See the report from the oral hearing preceding *Ligue des droits humains* in Thönnes, On Flights, Rock Concerts and the Needle in a Haystack, EU Law Analysis, 17 September 2021, https://eulawanalysis.blogspot.com/2021/09/on-flights-rock-concerts-and-needle-in.html, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

of mass surveillance technologies in the context of the ‘war on terror’ fundamentally changed the idea of the presumption of innocence.[96]

The CJEU’s PNR decision: recalibrating preventive security measures?

We focus here only on three points in *Ligue des droits humains* that relate to the preventive security dimension and different interpretations of what “preventive” may mean.

First, the application of the PNR Directive, where the Court distinguished between the internal and external dimension (intra-EU flights versus flights from third countries to the EU). In regard to the latter, the Court argued that the “very nature” of the threats would justify the systematic collection and transfer of PNR data to member states (see para 162). Excluding certain areas or groups of passengers would hamper the objective of the PNR Directive, namely, to identify persons who may present a risk to public security “from among all air passengers” (para 161). However, when it comes to intra-EU flights, the CJEU makes clear that a member state may only apply the PNR Directive if there are solid reasons to assume that it faces a genuine and present threat of serious crimes or terrorist offences. Moreover, the application of the PNR Directive to intra-EU flights must be strictly limited to the duration of the threat and to specific flight routes or airports (paras 171-172). The Court essentially uses a spatially stratified strict necessity test, which reflects two different meanings of “preventive security”. Internally, the Court requires a reasonable suspicion for the existence of a particular threat. The Court thus bends member states’ global preventive security logic towards a more targeted and reasoned logic of classical intelligence-led policing based on evidence in the EU . In other words, the application of the PNR Directive for intra-EU flights is conceptually viewed in the framework of policing security and not in terms of preventive security. Externally, the preventive security paradigm and general suspicion continue to reign.

Second, the CJEU considered, as it had already done in Opinion 1/15[97], that the collection of PNR data seriously interferes with the right to the protection of personal data under the EU Charter on Fundamental Rights. Any processing of PNR data must therefore be “strictly necessary” and limited to the purposes of the PNR Directive, that is, combating ‘terrorist offences’ and ‘serious crime’ (paras 148 et seqq.). In this regard, the CJEU was particularly

[96] For an example see Bigo/Guittet, Northern Ireland as metaphor: Exception, suspicion and radicalization in the ‘war on terror‘, 42 (2011), 483.
[97] CJEU, Opinion 1/15 of the Court [26 July 2017].

Electronic copy available at: https://ssrn.com/abstract=4547775

concerned about security and intelligence agencies using PNR data as mere search criteria for data mining in various other databases, and for other purposes than the PNR Directive intends. Therefore, the Court limited database interoperability: it made clear that the Passenger Information Units (PIUs) may compare PNR data only to databases on persons or objects sought or under alert (paras 182 et seqq.). Security and intelligence services are thus not permitted to process PNR data only because it gives them the possibility to nurture the predictive capacity of their databases.

Third, the willingness to predict through algorithms is based on the belief that the detection of anomalies or weak signals, which emanate from a small statistical group that shares the same characteristics, is only valid if the number of data initially collected is “large”. The systematic collection and storage of data over a long period of time is crucial for the functioning of any algorithm. This implies automatic processing of large amounts of data in which human intervention is limited to monitoring the process and intervening after sorting in a very limited number of cases. The Court, however, insists that human intervention must remain capable of understanding the specific reasons why an algorithm arrived at a positive match (para 210). The Court thus reintroduces a logic in which correlations are not enough to establish suspicion. Rather, causality is needed to establish ‘reasonable’ suspicion – and not a ranking in which many people may have high scores for bad reasons.

Conclusion

Instead of accepting a preventive security argument, the judges of the CJEU brought some reason into a derailed logic of collecting ever more data. In addition to curbing the expansion of preventive security, the PNR judgement may also help security services to enhance their efficiency and legitimacy. Security services do not seem to believe in Chris Anderson’s slogan that “data thinks for itself” and that we have reached “the end of theory because the flood of data is now making the scientific method obsolete”.[98] Rather, the work of security services is based on hypotheses, theories, research and evidence; in other words, on conjectural reasoning, as Carlo Ginzburg argues in his analysis of truth, history and security.[99]

[98] Anderson, The End of Theory: The Data Deluge Makes the Scientific Method Obsolete, Wired, 23 June 2008, accessible via: https://www.wired.com/2008/06/pb-theory/, last accessed: 23 June 2023.
[99] Ginzburg, Checking the Evidence: The Judge and the Historian, (1991) 18 Critical Inquiry, 79.

Electronic copy available at: https://ssrn.com/abstract=4547775

Contrary to studies that highlight the growing role of technologies in the design of an algorithmic security apparatus organised around quantitative techniques of knowledge production, Laurent Bonelli and Francesco Ragazzi show that the heart of counter-terrorist intelligence gathering is largely a matter of using qualitative and analogical techniques: informants, interpersonal relationships and the operationalisation of knowledge through traditional methods such as writing reports, notes and summaries.[100]

Ligue des droits humains thus offers an opportunity for national judges to question more radically the idea of generalised preventive security that seeks to anticipate human behaviour through the creation of risk profiles and statistical correlations (instead of causality). Judges should question more directly the idea of preventive security and seek clarifications on what constitutes ‘reasonable suspicion’. For without proper justifications, ‘reasonable suspicion’ is kind of an oxymoron.

[100] Bonelli/Ragazzi, Low-tech security: Files, notes, and memos as technologies of anticipation, (2014) 45 Security Dialogue, 476.

Electronic copy available at: https://ssrn.com/abstract=4547775

Caution: Safeguards may appear more robust than they are

Thorsten Wetzling

When public authorities collect and process personal data, they interfere with people's fundamental rights and freedoms. For such interferences to be deemed lawful by European Courts, they need to be limited to what is necessary in a democratic society and subject to effective review by a court or an independent administrative body.[101] So far, so clear. Yet, what does this mean in actual practice? European and national lawmakers often grapple with this question when they draft or amend security and surveillance legislation.

At a time when the European security architecture is evolving, and when national lawmakers must pay greater attention to an evolving set of common standards and safeguards to prevent disproportionate government access to data, it is essential to shed critical light on their implementation in actual practice. This post attempts to do this by examining the EU PNR Directive[102] and the German legal framework on bulk collection.[103] As different as these frameworks for untargeted surveillance are, they both include provisions that seek to prevent disproportionate government access and to ensure effective and independent review of data collection and subsequent data processing. This post tells a cautionary tale of good and less good attempts at meeting these important objectives by honing in on a few exemplary provisions and by discussing corresponding court findings thereon.

The good news

Lawmakers deciding over the general competence of public authorities to use untargeted surveillance instruments and the design of 21st-century oversight and accountability mechanisms can find a wealth of guidance in recent jurisprudence of the Court of Justice of the EU (CJEU) and the European Court of Human Rights (ECtHR), as well as landmark judgments by national courts. This evolving case law now provides a far more granular articulation of permissible objectives and common safeguards against executive overreach. In turn, this allows

[101] See the ECtHR's Factsheet on Mass surveillance, accessible via: https://www.echr.coe.int/documents/d/echr/fs_mass_surveillance_eng, last accessed: 26 June 2023.
[102] Directive (EU) 2016/681, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0681, last accessed: 26 June 2023.
[103] See the German Act on the Federal Intelligence Service (*Bundesnachrichtendienstgesetz*), accessible via: https://www.gesetze-im-internet.de/bndg/, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

for clearer orientation and should facilitate lawmakers' delicate calibration of rights and interests.

Constant challenges

Caution is still needed, however, because the grown European repository does not prescribe specific practices. Rightly, this remains the responsibility of legislatures across Europe. When lawmakers take on the difficult task to refine and expand existing oversight and accountability mechanisms in accordance with the repository, the challenge remains that such mechanisms need to be adequately resourced, practised and (re-)evaluated. Else, practice on the ground stands no chance to approximate the rules on the books. Furthermore, lawmakers enjoy substantial room for manoeuvre when implementing specific aspects of the repository. This, too, can bear several risks: As judgments typically proclaim only minimal standards, additional guardrails may be needed to ensure an independent and effective review of the use of fast-evolving technology. Moreover, lawmakers can avail themselves of too much constructive ambiguity in the drafting process: They might use vague language that, while conveying adherence to a certain safeguard, leaves practitioners too much leeway to pay only lip service to a particular requirement. As some examples discussed below show, a mere gestural implementation of the European repository runs counter to its overall objective.

Effective trimming of surveillance powers

Before turning to underwhelming practice, consider first the CJEU's review of the EU's PNR Directive[104], and recitals 183-188 of the judgment more specifically. It is where the CJEU sets an effective limit on the universe of databases that can be made available to Passenger Information Units (PIUs). According to Article 6 (3) (a) of the Directive, "the PIU may 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 […]“. The Court rightly identified a key problem of this provision: It does not specify which other databases could be considered 'relevant' in the light of the objectives mentioned. Given that Article 6 (3) (a) of the Directive does not expressly indicate the nature of the data that those databases may contain, or their relationship to the stated objective, the CJEU terminated this open-endedness to ensure that the PIU's access to

[104] See CJEU, Case C-817/19 *Ligue des droits humains* [21 June 2022].

Electronic copy available at: https://ssrn.com/abstract=4547775

personal data is not disproportionate. In so doing, it sets an effective limit as regards the amount of databases that PIU's can avail themselves for PNR comparisons: they can only use databases on persons or objectives sought or under alert (CJEU decision, paras 187-188). Without such exemplary trimming of this particular surveillance provision in the PNR Directive, the databases in question could have included a wide universe of information drawn from various collection methods, including but not limited to Open Source Intelligence and Social Media Intelligence. Rightly, the CJEU also addressed a grave concern and open question related to the management of such databases by private entities: They rarely are accountable to the same standards as public authorities.

Effective oversight empowerment

Another powerful advancement of the European repository occurred when the German Federal Constitutional Court (Bundesverfassungsgericht, hereafter BVerfG) decided in May 2020, that large tenets of the German foreign intelligence legislation were unconstitutional.[105] This landmark judgement caused a major redesign and empowerment of intelligence oversight in Germany.[106] Among the long list of deficits that the Court identified was an unduly strict interpretation by the German Government of the so-called third party rule. "[A]ccording to this rule, based on informal arrangements, intelligence obtained from foreign intelligence services may not be shared with third parties without the consent of the intelligence service in question" (BVerfG judgment para 293). The Court argued that independent and effective review of surveillance practices was too often torpedoed, or substantially impaired, because of the untamed application of this rule in actual practice. Clarifying that the third party rule is "an administrative practice that is not legally binding, but is merely based on agreements with other intelligence services" (BVerfG judgment, para 294), the Court then held that "it is thus flexible and […] in the future, it must be ensured, through the way the oversight bodies are designed and through changes in agreements with foreign services, that the bodies conducting legal oversight are no longer considered "third parties" (Ibid).

[105] See BVerfG, Decision of 19 Mai 2020, 1 BvR 2835/17, BVerfGE 154, 152, accessible via: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2020/05/rs20200519_1bvr283517.html, last accessed: 26 June 2023.

[106] See Stiftung Neue Verantwortung, Ditlmann/Wetzling, Caught in the Act? An analysis of Germany's new SIGINT reform, 25 November 2021, accessible via: https://www.stiftung-nv.de/sites/default/files/caught-in-the-act_analysis-of-germanys-new-sigint-reform_0.pdf, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

In response to this judgment, the Bundestag created a powerful new judicial intelligence oversight body.[107] It also had to make sure that it enjoyed comprehensive access to all premises, IT systems and operational databases of the foreign intelligence service and that "the Federal Intelligence Service cannot prevent oversight by invoking the third party rule" (BVerfG judgment para 85). As discussed in further detail below, this exemplary trimming of surveillance practice and bolstering of effective oversight should be born in mind when assessing decisions on legal frameworks, such as the PNR Directive, where important surveillance decisions are said to be "open to effective review by a court or independent administrative body" (CJEU decision, para 172).

Less effective safeguards against disproportionate government access to data

Yet, one can also find ample proof of less effective implementations of the growing European repository in actual practice. Consider, for example, the CJEU's findings regarding the "[s]afeguards surrounding the automated processing of PNR data" (CJEU judgment paras 202-213) and the rather vague documentation requirement of PIU activities this context.

Recurring to recital 7 and Articles 6(5) and (6) of the PNR Directive, the Court summarises that PIUs are required to:

- "define assessment criteria in a manner that keeps to a minimum the number of innocent people wrongly identified by the system established by the PNR directive";

- "individually review any positive match by non-automated means in order to identify to, as much as possible, any false positives";

- "carry out a review for the purpose of excluding any discriminatory results" (CJEU judgment paras 203).

Referring to "Article 6(5) and (6) of the PNR Directive, read in conjunction with recitals 20 and 22 thereof", the Court further underlines that Member States have important responsibilities regarding the implementation and review of these obligations. More specifically, they must:

[107] The so-called 'Unabhängiger Kontrollrat', see https://ukrat.de/DE/Home/home_node.html, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

- "lay down clear and precise rules capable of providing guidance and support for the analysis carried out by the agents" (CJEU judgment para 205);

- "ensure PIUs establish in a clear and precise manner objective review criteria enabling its agents to verify whether positive match concerns effectively individual who may be involved in terrorist offenses / serious crime, but also non-discriminatory nature of automated processing"; (Ibid., para 206) and

- "ensure that PIUs maintain documentation relating to all processing of PNR Data carried out in connection with the advance assessment" (Ibid., para 207).

Ill-defined documentation requirements invite creative non-compliance and prevent effective audits

Consider just the last point. The vagueness of the documentation requirement is striking. This should have been spelled out more specifically in the Directive, and, by extension, the Court. This is because some documentation practices are clearly more conducive to effective review by supervisory authorities than others. Vaguer documentation requirements constrain the supervisory authorities' access to relevant information. Put differently, they leave considerably more room for creative non-compliance by the PIUs. Hence it is important to know whether reviewers have comprehensive or only cursory access to the log files of the PIUs. Can they access this information directly or remotely? Depending on the answer to these questions, reviewers might benefit tremendously from automated control programs.[108] In turn, this may significantly improve the ability of auditors to assess the legality and (provided their review mandate allows for it) the effectiveness of the data processing.

Unfortunately, the rather unspecified documentation requirement in the PNR Directive seems to have passed the CJEU's scrutiny. As a result, the documentation requirement seems more gestural in nature. For it to be an effective safeguard, there needs to be further mention of comprehensive access and investments and use of supervisory technology.

[108] Stiftung Neue Verantwortung, Vieth/Wetzling, Data-driven Intelligence Oversight, November 2019, accessible via: https://www.stiftung-nv.de/sites/default/files/data_driven_oversight.pdf, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

Merely "being open to effective review" is not enough

Another more gestural limitation of surveillance powers in the PNR Directive is tied to the way in which supervisory authorities are positioned to review the existence of a terrorist threat. Take situations where the signatories of the EU PNR Directive conclude "that there are sufficient solid grounds for considering that it is confronted with a terrorist threat that is shown to be genuine, present or foreseeable" (CJEU judgment, para 171). In such situations, according to the Court, Member States may decide, for a limited period of time, to apply the PNR Directive regime also to all intra-EU flights (Ibid., para 173). The CJEU stipulates, however, that this decision must be "open to effective review by a court or independent administrative body, whose decision is binding in order to verify that the situation exists, and that conditions and safeguards which must be laid down are observed" (Ibid., para 172).

This important safeguard may encounter significant difficulties when it comes to its implementation, however. For example, a review body may simply lack the competence, ability or resources necessary to independently "verify" whether a terrorist threat is shown to be genuine, present and foreseeable. Moreover, and tied to this, key information needed for this assessment may not originate from the Member State facing a terrorist threat. As previously discussed, supervisory authorities of a Member State may be prevented from seeing the data due to national restrictions, for example unduly strict national interpretations of the 'third party rule'.

Furthermore, an oversight body's formal mandate may be limited to the assessment of the legality of a surveillance measure. Depending on national regulations, this may not include an independent verification whether the executive has sufficiently justified that a particular threat to the country is genuine, present and foreseeable. In addition, supervisory authorities across Europe have seen a remarkable increase in tasks that new legislation attributed to them. Apart from the necessary financial resources and technical equipment, supervisory authorities may simply lack the time or motivation to take on additional tasks. Thus, when planning new audits and inspections, some understandably tend to focus first and foremost on their formal remit. As a result of this, the mere fact the PNR Directive proclaims that important surveillance decisions are 'open to effective review' may not necessarily mean that they are going to be reviewed, let alone effectively.

Collusive delegation: The undesirable side effect of trimmed surveillance?

Electronic copy available at: https://ssrn.com/abstract=4547775

Let us revisit the German legal framework on foreign intelligence collection at the end of this cautionary tale. This will be done to caution against another potential form of accountability evasion that is likely to be found in other jurisdictions, too. More specifically, the ensuing discussion will show that the trimming of an agency's surveillance powers will not prevent disproportionate processing of data if another, less regulated, agency is allowed to take over.

Reference is made to §24 (7) of the German BND Act. It embodies an important exception to the general restriction that content data may only be collected in bulk on the basis of search terms. Due to this exception, Germany's foreign intelligence service may perform so-called suitability tests. This is done in order to test the suitability of specific telecommunication networks for bulk collection purposes or to generate new search terms or to assess the relevance of existing search terms. Some tests do not require a written order by the president of the BND and there is no requirement, as in other democracies[109], to involve independent oversight bodies in the process. Equally problematic, neither the duration nor the volume of the data collected in pursuit of suitability tests is subject to effective limitations.[110] Even worse: According to §24 (7) of the BND Act, Germany's foreign intelligence service may share an unrestricted amount of data it has collected in this way automatically with unspecified intelligence units within the German Armed Forces. Given that the various forms of data processing by the intelligence units of the German Armed Forces are nowhere near as strictly regulated, let alone independently overseen, this provision incentivizes what political scientists call collusive delegation. Agents who reportedly complain about an unduly restricted surveillance regime[111] may rely on this provision to share more data with the Armed Forces not just because this is deemed necessary, but because its data processing is subject to fewer restrictions. This would clearly run counter to the European repository's core objective and heeds a warning to lawmakers to adopt a functional or inter-agency approach when it comes to the implementation of the European repository. This, by the way, is also a central demand of the Council of Europe's modernised Convention 108.[112]

[109] See https://www.intelligence-oversight.org/countries/new-zealand/, last accessed: 26 June 2023.

[110] Wetzling, Statement in front of the German Bundestag Committee on Internal Affairs regarding the reform of the BND Act, accessible via: https://www.bundestag.de/resource/blob/823556/760abb7961fa7df144e1bc834702d44f/A-Drs-19-4-731-F-data.pdf, last accessed: 26 June 2023.

[111] Bewarder/Flade, Lauschangriff? Erlaubt!, Tagesschau, 21 April 2023, accesible via: https://www.tagesschau.de/investigativ/ndr-wdr/bnd-unabhaengiger-kontrollrat-101.html, last accessed: 26 June 2023.

[112] Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Opinion on the Data protection implications of the processing of Passenger Name

Electronic copy available at: https://ssrn.com/abstract=4547775

Conclusion

This post focused on a complex and ongoing challenge for many lawmakers across Europe: How to effectively implement the growing repository of European standards, norms and safeguards against disproportionate government access when amending or adopting new laws? The discussion shows that the risk of ineffective or gestural trimming of untargeted surveillance powers and ineffective review remains genuine. Yet, as the first two examples testify, there is also much progress and past mistakes are being rectified, too.

While ridding liberal regimes from illiberal practices requires constant work in progress, it is well worth the effort. It is what will distinguish the growing European security architecture from authoritarian regimes.

Records, T-PD(2016)18rev, 19 August 2016, accessible via: https://rm.coe.int/16806b051e, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

The European Legal Architecture on Security

Elspeth Guild, Tamás Molnár

New Developments in the Complex Relationship Between the Public and Private Sectors in Data Processing

As the European legal architecture on internal security is being built around large-scale databases[113], AI tools and other new technologies, the relationship between the public and private sectors has become increasingly complex. In this blog, we examine one aspect of the Court of Justice of the European Union (CJEU)'s recent judgment in *Ligue des droits humains*[114], namely the data protection rules applicable to cooperation between the public and private entities in personal data sharing.

As the private sector (e.g. banks, telecommunications companies) has, in many cases, outstripped the public sector in personal data collection and use, when the public sector seeks more information on people for criminal justice or internal security purposes, it increasingly requires the private sector to share personal data with it (e.g. in the field of anti-money laundering[115]). Similarly, as data processing tools in the private sector have been developed and perfected for commercial purposes which enhance knowledge about individuals, the public sector has sought to capitalise on these increasing capacities, by requiring private sector entities to share results of personal data analyses.

The legality of both personal data and analysis sharing between the private and public sectors depends on compliance with EU data protection rules. Two legal regimes apply in parallel: First, the General Data Protection Regulation (GDPR)[116], which places the individual's right to data autonomy at the centre. Second, the Law Enforcement Directive (LED)[117], which provides for personal data use in the field of prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties, including the safeguarding against

[113] Bellanova/Glouftsios, Formatting European security integration through database interoperability, (2022) 31 European Security, 454.
[114] CJEU, Case C-817/19 *Ligue des droits humains* [21 June 2022].
[115] See https://finance.ec.europa.eu/financial-crime/eu-context-anti-money-laundering-and-countering-financing-terrorism_en#legal, last accessed: 26 June 2023.
[116] Regulation (EU) 2016/679, accessible via: https://eur-lex.europa.eu/eli/reg/2016/679/oj, last accessed: 26 June 2023.
[117] Directive (EU) 2016/680, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

and the prevention of threats to public security. The LED provides for exceptions to the strict rules on data autonomy which otherwise apply as a result of the GDPR.

In this blog post, we set out the challenges to both the public and private sectors regarding data transfers in the context of the cross-border movement of persons, in particular by air. We examine the issue of private transport sectors' access to and collection of personal data, to which public authorities have less direct access, and the crystallisation of duties on the private transport sector to share this data with the public sector based on the Passenger Name Record (PNR) Directive.[118] We explore the interpretation of the PNR Directive by the CJEU, which establishes clear lines on where each of the data protection standards lay. We conclude that the CJEU has protected the private sector from demands for data sharing by the public sector, which go beyond that permitted by the GDPR (unless the public sector can justify the demand on LED grounds). The judgment thus enhances the 'personal data autonomy' of individuals and requires public authorities to justify to a high standard any obligations it seeks to place on the private sector to share personal data related, directly or indirectly, to travel by air.

It Has Always Been a Bumpy Road: The Evolution of EU Law before the Ligue des Droits Humains Ruling

Large quantities of personal data are collected by the private sector in the normal pursuit of their business activities, and in that context, much of it is stored for varying periods for contractual purposes. Nowhere is this more evident than in the case of telecommunications companies and internet platforms, where subscribers provide their personal data most consciously for service provision and billing purposes, and the companies retain this data for provision and invoicing purposes. Less consciously, on the part of the consumer, and more controversially, internet platforms and other social media companies collect personal data about their customers from their use of the company's tools and sell this onwards to make the activity profitable.

The interest of state authorities to access these (invaluable) sources of personal data for security-related purposes has developed as rapidly as the databases themselves. In 2014, the CJEU found that an EU Directive[119], which required telecoms providers to stock and make

[118] Directive (EU) 2016/681, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0681, last accessed: 26 June 2023.
[119] Directive 2006/24/EC.

Electronic copy available at: https://ssrn.com/abstract=4547775

available on request to national law enforcement authorities personal data of their customers, was incompatible with the Charter of Fundamental Rights of the EU (Digital Rights Ireland[120]). This judgement began a reappraisal of the relationship between private sector actors and EU law enforcement authorities, as regards the processing and transferring of personal data, the right to privacy and data protection considerations.

In 2017, the CJEU was once again faced with a case where the private sector, in the form of airlines and their agents, were required by state authorities to provide personal data about their customers for law enforcement purposes (fighting terrorism and other forms of serious crime). The issue challenged was the EU-Canada Passenger Name Record (PNR) Agreement of 2006, which required airlines (or their agents, as the collection and storing of PNR data is normally carried out by companies contracted by airlines for this purpose) to make available all PNR data on passengers travelling to Canada for the purpose of preventing and combating terrorism and related crimes and other serious crimes that are transnational in nature, including organised crime. In its Opinion 1/15[121], the CJEU did not find that the bulk transfer of data was contrary to the Charter rights to privacy and data protection. However, it did find that in so far as the agreement did not preclude the transfer of sensitive data from the EU to Canada and the use and retention of that data, it was incompatible with those Charter rights.

The CJEU's Stance in Ligue des Droits Humains on Private/Public Collaboration in Data Transfers

In 2022, the CJEU was again faced with a challenge to the legality of the transfer of PNR data from airlines and their agents to state authorities (for the same law enforcement purposes as above), this time contained in the 2016 PNR Directive. Central to this judgment (*Ligue des droits humains)* was the data protection standards applicable to such transfers of personal data from the private sector to state authorities. The judgement is of great importance generally to the internal security-related legal architecture of the EU, many aspects of which are considered in other contributions to this blog series. Here we only examine the issue of personal data sharing between the private and public sectors.

The PNR Directive requires personal PNR data sharing by private actors with state competent authorities (law enforcement), exclusively for the purposes of the fight against terrorism and

[120] CJEU, Cases C-293/12 and C-594/12 *Digital Rights Ireland* [8 April 2014].
[121] CJEU, Opinion 1/15 of the Court [26 July 2017].

Electronic copy available at: https://ssrn.com/abstract=4547775

other forms of serious crime (Article 1(2)). The question referred to Luxembourg was on the correct legal basis in EU data protection law for such transfers. For the purposes of the competent law enforcement authorities, in so far as the use of the data is limited to action in respect of terrorism and serious crime, the EU's Law Enforcement Directive is applicable. This Directive requires that personal data is processed lawfully, collected for specific, explicit and legitimate purposes and is not excessive in relation to the purpose for which it is processed (Article 4). However, in view of the subject matter of the Directive (i.e., data processing for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties), competent authorities in law enforcement have wider powers to collect and use personal data than private sector actors do, and there are fewer rights for the data subjects.

The data protection rules applicable to the private sector and state authorities not carrying out law enforcement activities as defined in the LED are set out in the GDPR, which allows for much more limited grounds for data collection, storage, use and transfer, coupled with higher safeguards for the data subjects. The exceptions which Member States can make to the applicable rules are strictly set out in Article 23, accompanied by areas carved out of its material scope (Article 2(2)). The question arose as to which EU legal regime was applicable to PNR data collected by the private sector and transferred in bulk to state competent law enforcement authorities. A related question was whether or not the PNR Directive can be regarded as a purely lex specialis instrument on data transfers and data protection, setting out self-standing standards independently from the above-mentioned horizontal pieces of EU data protection acquis.

The CJEU found that private sector actors (here: air carriers and their agents) – as entities not exercising public authority and not being entrusted with public powers – are obliged to fully comply with the GDPR. They cannot carry out data collection or processing operations, which can only be justified on the grounds of law enforcement exceptions in the LED. Secondly, data transfers from private sector actors to the competent state authorities (the Passenger Information Units – PIUs) can only take place in accordance with the GDPR. In all circumstances, the exception in Article 23(1)(f) GDPR (transfer for the 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) must be interpreted consistently with the rights to privacy (Article 7) and protection of personal

Electronic copy available at: https://ssrn.com/abstract=4547775

data (Article 8) in the Charter. Finally, the PIUs – and other competent law enforcement agencies within the meaning of the PNR Directive – must process the transferred personal data in accordance with GDPR rules unless there is a criminal justice (terrorism or serious crime) objective – in that case, the LED rules apply. The objective for which the PIUs process personal data will depend on the requests from competent authorities. Logically, this also means that if the law enforcement authority is an intelligence service under domestic law and the objective of data processing is fighting terrorism, the LED will apply – at least this flows from the CJEU's *Ligue des droits humains* ruling. Reading Articles 2(2) and 3(7) LED in conjunction also supports this interpretation. Importantly, private sector actors cannot be asked to carry out processing actions which can only be authorised under the LED. Their duties all exclusively fall within the remit – and the higher data protection standards – of the GDPR. This is where we stand now regarding privacy protection obligations under multiple EU instruments.

Lessons for the Reform of Advance Passenger Information

With the above, the CJEU clarified, walking in the footsteps of the La Quadrature de Net jurisprudence[122], that when private entities and law enforcement authorities collaborate in mass data transfers and processing of personal data, a peculiar mix of standards and safeguards stemming from different strands of EU data protection legislation regulate such scenarios. Clear lines of data protection duties determine various steps of such collaboration. The PNR Directive may be seen as only partially constituting lex specialis, which blends the GDPR and the LED with some "own" PNR-specific standards regulating data processing and protection by both private and public actors.

Arguably, the lessons learnt for the data protection boundaries of private/public collaboration do not stop here. When zooming out and taking a broader look at the ramifications of the CJEU ruling, its implications on the future collection and processing of Advance Passenger Information (API) under EU law come to mind first, as the CJEU was explicitly asked to give authentic guidance on the applicable data protection regimes in this context, too. As regards processing API data, the CJEU closed the door on the applicability of the LED. In view of the core purposes of collecting API data, which are reinforcing border controls and curbing irregular migration, all API-related data processing operations must be governed by the GDPR.

[122] CJEU, Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net* [6 October 2020].

Electronic copy available at: https://ssrn.com/abstract=4547775

The LED only applies when API data is used and processed for law enforcement purposes as defined in national law (Article 6(1) of the API Directive[123]).

Another related intriguing question is to what extent the European Commission' new proposals[124] reforming the use of API data across the Union tally with the CJEU's findings applicable to the processing of API data. But this assessment is a story for another day. Until then and while pondering more generally on how to strike the fair balance between state security interests and the protection of fundamental rights of millions of data subjects, the wise caution by Advocate General Pitruzzella in the CJEU case at hand may echo in our ears: "[here] we have a contemporary twist on a classic theme of constitutionalism since, as The Federalist categorically asserted, men are not angels, which is why legal mechanisms are needed to constrain and monitor public authorities."[125]

[123] Council Directive 2004/82/EC, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004L0082, last accessed: 26 June 2023.
[124] See https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7644, last accessed: 26 June 2023.
[125] Opinion of Advocate General Pitruzzella, C-817/19 *Ligue des droits humains* [27 January 2022], p. 4.

Electronic copy available at: https://ssrn.com/abstract=4547775

Foreseeability and the Rule of Law in Data Protection after the PNR judgment

Amanda Musco Eklund, Magdalena Brewczyńska

In his seminal book titled "The Morality of Law", Lon L. Fuller explained that, among other things, the rule of law cannot be reconciled with the existence of secret laws, unclear laws and laws which cannot be obeyed.[126] Yet, these seemingly straightforward postulates may turn out to be surprisingly difficult to realize in practice. This is especially the case in the regulatory areas where full transparency is at odds with the legislative goals; where a certain degree of flexibility of rules is necessary to address changing circumstances, in which these rules function; and where a disconnect occurs between the visions of the lawmaker and reality created by modern technologies that are utilized to pursue them.

In the following, we reflect on the Passenger Name Record Directive (PNR Directive)[127], as recently interpreted by the Court of Justice of the European Union (CJEU) in the *Ligue des droits humains*[128] judgement, from the perspective of the aforementioned postulates concerning the rule of law. The CJEU was requested to respond to a number of pertinent questions regarding the asymmetry of powers provided by the PNR Directive in relation to individuals, whose personal data and privacy are at stake by the processing of PNR data. In this contribution, we will focus specifically on how the Court addressed the problem of foreseeability of measures established under the PNR Directive. We argue that the Court shared the concern about the PNR system's compliance with the rule of law, but failed to provide conclusively guidance on what minimum criteria to demand of the quality of the law that governs modern security measures.

The PNR Directive and Asymmetry of Powers

The PNR Directive provides for the collection and transfer of PNR data of passengers of extra-EU flights by air carriers to the designated state institutions, namely the Passenger Information Units (PIU), and the processing of the PNR data by Member States, as well as exchange of PNR data between Member States. By imposing the obligation on the air carriers to collect and

[126] Fuller, The Morality of Law (Yale University Press 1969).

[127] Directive (EU) 2016/681, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0681, last accessed: 26 June 2023.

[128] CJEU, Case C-817/19 *Ligue des droits humains* [21 June 2022].

Electronic copy available at: https://ssrn.com/abstract=4547775

transfer information for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, the EU legislator made the air carriers an important link in the chain of modern security architecture. This architecture is characterized by the ever-increasing role of private actors in contributing to the performance of law enforcement and security tasks by the state. The joint-forces of public and private actors create a new social reality, in which an individual is no longer confronted only with the power of the state, but with a network of power created by both the state and non-state actors. This implies that the protection traditionally afforded by the rule of law standards, such as foreseeability of coercive measures, needs to reach beyond the state-individual relation and take account of the third player in this picture: the private actors.

The Role of Private Actors and the Foreseeability Requirement

The foreseeability of fundamental rights interferences is relevant when private actors provide the public decision-maker with personal data, which then becomes automatically processed by public bodies. In the case of the PNR Directive, the national PIUs carry out automated risk analyses of the personal data provided by the air carriers – both by comparing it to ‘relevant databases’ and against pre-determined risk criteria – and any positive match is individually reviewed by non-automated means by the Member States’ PIUs (Article 6).

The requirement of foreseeability is a substantive part of the principle of legality, which in essence is a limit to the exercise of public power, and strives to ensure that powers are sufficiently defined in order for its exercise to be foreseeable to individuals and not arbitrary. In the judgement, the principle of legality is discussed under the assessment of Article 52(1) of the Charter, which concerns the legality requirements on fundamental rights limitations. According to this provision, legal rules must have a certain level of foreseeability for interferences in the rights to privacy and data protection to be “provided for by law”.

Foreseeability is a rule of law requirement which does not rest on private actors, but on the public in its exercise of power. However, the regulation and interpretation of how private actors can transfer personal data to public actors is central to this public requirement on exercise of power, as it affects the foreseeability and legality of these public actors’ automated processing.

In general, any lack of clarity regarding the rules and safeguards applicable to the processing by private actors and their collaboration with the public leads to a lack of clarity when it comes to what kind of data will be used for the public automated processing and the subsequent

Electronic copy available at: https://ssrn.com/abstract=4547775

decision-making. Therefore, if the outcome of semi-automated decision making is unforeseeable due to the involvement of private actors, that becomes a rule of law problem.

Quality of Law Requirements

It is not sufficient for the Court that there are formal legal grounds for processing, since, tacitly following Fuller[129], the Court also takes account of a quality of law test related to clarity and foreseeability. This is expressed by the Court in the judgement in terms of requiring that an act permitting interferences with rights "must itself define the scope of the limitation on the exercise of the right concerned" and that the legislation must lay down "clear and precise rules governing the scope and application of the measures provided for".[130]

In the judgement, the Court finds that the legality requirement is satisfied, stating that the PNR Directive lists PNR data and provides a detailed framework for processing those data. However, as the Directive was formulated, not all provisions met the requirement of clarity and precision according to the Court. For example, provisions on what PNR data the air carriers are obliged to provide (paras 129 et seq.) or what constitutes 'relevant databases' which may be compared against PNR data (paras 182 et seq.). This led the Court to clarify those provisions itself, as the Court may specify legislation by interpretation.

The Court does not develop much on, or criticize, the clarity and precision of the legal basis for the collaboration with private air carriers. Instead, the Court mainly clarified when the General Data Protection Regulation[131] or Law Enforcement Directive[132] applies (paras 77–84). The main problem, as has been discussed in previous research (see e. g. Purtova[133]; Gottschalk[134]; Brewczyńska[135]), is that the different applicable legal regimes offer substantially different data protection standards. On a practical level, in the context of public private collaborations, the duality of legal regimes may also lead to confusing situations, where

[129] Fuller, The Morality of Law (Yale University Press 1969).
[130] CJEU, Case C-817/19 *Ligue des droits humains* [21 June 2022], paras 114, 117.
[131] Regulation (EU) 2016/679, accessible via: https://eur-lex.europa.eu/eli/reg/2016/679/oj, last accessed: 26 June 2023.
[132] Directive (EU) 2016/680, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680, last accessed: 26 June 2023.
[133] Purtova, Between the GDPR and the Police Directive: Navigating Through the Maze of Information Sharing in Public-Private Partnerships, (2018) 8 International Data Privacy Law, 52.
[134] Gottschalk, The Data-Laundramat?, (2020) 6 European Data Protection Law Review, 21.
[135] Brewczyńska in Kosta/Leenes/Kamara (eds), Research Handbook on EU Data Protection Law (Elgar 2022), 91.

Electronic copy available at: https://ssrn.com/abstract=4547775

different standards apply to the same sets of data, depending on the purpose of the processing and type of entity carrying out the processing.

Another problematic aspect, looking generally at the implementation of regimes involving automated analysis of personal data, is that they are based on software which has rarely only been developed by the public body using them. The design of software, such as risk screening algorithms, and the choices made in that process, are essential to the decision-making process. Hiring private actors to do this could be considered a form of de facto delegation, which raises questions on monitoring, foreseeability and accessibility.[136]

Further Down the Road: The Foreseeability of Automated Processing

In the judgement, the Court considers that the rules on automated processing are sufficiently detailed. When the Court defines what is clear and precise – as it did here – this sets a standard for future automated processing in the European security architecture. One may question whether the rules on automated processing in the PNR Directive are clear and precise enough to be sufficiently foreseeable, considering the new challenges related to opacity which comes with automation of public decision-making.

The judgement allows for quite a lack of foreseeability and wide discretion as regards the establishment of pre-determined risk criteria. This is central, as – together with the personal data – the risk criteria are the main components of automated risk assessments (Article 6(3)). What triggers a hit is a correlation between these two components, which is a very different foundation for decision-making than causality (see Bayamlıoğlu and Leenes).[137] As the Court held, the extent of the interference of automated analysis of PNR data essentially depends on the pre-determined models and criteria (para 103).

The limits to the establishment of pre-determined risk criteria are held in general terms in the judgement and Directive: they must be specific, non-discriminatory, targeted and proportionate (paras 105, 189; Article 6(4)). These generic limitations leave wide discretion to the actor who gets to define these risk indicators in non-accessible and often secret acts, which is what Fuller is sturdily warning against.[138] In the PNR regime, the defining actor is the national PIU.

[136] Hofmann, An Introduction to Automated Decision-Making (ADM) and Cyber-Delegation in the Scope of EU Public Law, University of Luxembourg Law Research Paper No. 2021-008, p. 20.
[137] Bayamlıoğlu/Leenes, The ‘rule of law’ implications of data-driven decision-making: a techno-regulatory perspective, (2018) 10 Law, Innovation and Technology, 295.
[138] Fuller, The Morality of Law (Yale University Press 1969).

Electronic copy available at: https://ssrn.com/abstract=4547775

Parallels can also be drawn to the upcoming IT-system ETIAS[139], which provides for similar automated risk screenings of visa-exempt third-country nationals, but where the EU agency Frontex will finally establish the pre-determined risk criteria.[140] While the requirement that risk criteria must be non-discriminatory is not developed in depth here, it should be underlined that this requirement in itself represents a challenge for the actors defining risk criteria, as previous research has stressed the risk of discriminatory profiling (both direct and indirect by proxy) which comes with using personal data for automated risk-profiling systems.[141]

Rule of Law Implications on the European Security Architecture

When balancing the right to privacy and data protection of the individual against the public interest of security, one problematic aspect is what seems to be a rising logic of the automated European security architecture. The CJEU relies heavily on the proper functioning of subsequent manual processing to correct the inherent issues and margin of errors which come with automated processing (paras 123–124). This overlooks that while manual assessment is considered an additional safeguard against fully automated decision-making, it also constitutes a form of heightened surveillance of certain individuals. Not only the final manual decision of a PIU matters, as the automated filtering constitutes an important de facto decision in an automated decision-making process[142], particularly as only those filtered out by the automated processing are subject to further checks.

100% foreseeability is not reasonable to expect in a security context where full transparency is at odds with the legislative goals, and a certain degree of flexibility of rules is necessary. However, there seems to be a new logic in this automated context of what can justify a fundamental rights interference. It is not a person’s behavior, or any reasonable suspicion that subjects you to the first interference, but simply being a passenger, or in the case of the ETIAS regime, being a third-country national from a visa-exempt country. ‘Reasonable suspicion’, in this risk-based approach, is replaced by other triggers for interferences: who you are, in the

[139] Regulation (EU) 2018/1240, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1240, last accessed: 26 June 2023.

[140] Musco Eklund, Frontex and ‘Algorithmic Discretion‘ (Part I), Verfassungsblog, 10 September 2022, https://verfassungsblog.de/frontex-and-algorithmic-discretion-part-i/, last accessed: 26 June 2023.

[141] Vavoula, Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism, (2021) 23 European Journal of Migration, 457; Derave/Genicot/Hetmanska, The Risks of Trustworthy Artificial Intelligence: The Case of the European Travel Information and Authorisation System, (2022) 13 European Journal of Risk Regulation, 389.

[142] Binns/Veale, Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR, (2021) 11 International Data Privacy Law, 319.

Electronic copy available at: https://ssrn.com/abstract=4547775

case of ETIAS, which base risk indicators on data such as education level, age and occupation (Arts. 17(2), 20(5)), or how you travel, in the case of the PNR directive (Annex 1).

The PNR judgment illustrates an approach where less foreseeability will be accepted in the regulatory area of automated security and border control. This should be critically discussed from a rule of law perspective in light of automated systems' opacity challenges, as automation arguably instead calls for a higher level of foreseeability to uphold rule of law safeguards. As stated by the Court: "The need for such safeguards is all the greater where personal data are subject to automated processing" (para 117).

Foreseeability and Room for Legal Interpretation

Legal rules must be clear and precise to ensure "that situations and legal relationships remain foreseeable"[143] (Venice Commission, Report on the Rule of Law, para 46). In the discussed judgement, however, the CJEU attributed a considerable value to the role of interpretation. The Court emphasized the need for interpreting the PNR Directive, as far as possible, in a way, that would not affect its validity and conformity with primary law and, in particular, with the provisions of the Charter (para 86). Furthermore, "when a directive allows the Member States discretion to define transposition measures adapted to the various situations possible, they must, when implementing those measures, not only interpret their national law in a manner consistent with the directive in question but also ensure that they do not rely on an interpretation of the directive that would be in conflict with the fundamental rights protected by the EU legal order or with the other general principles recognized by EU law" (para 87).

This approach may bring into doubt the PNR Directive's compliance with the standards of clarity and precision. On the one hand, as discussed earlier, the Court seems to notice several shortcomings of the PNR Directive in the *Ligue des droits humains* decision. On the other hand, it attempts to mitigate them by calling upon a pro-Charter interpretation, thereby leaving individuals whose privacy and personal data are concerned 'at the mercy' of the good will of the Member States. This further includes the challenging responsibility Member States face to establish non-discriminatory risk criteria, as mentioned above.

[143] Venice Commission, Report on the rule of law, CDL-AD(2011)003rev-e, 25-26 March 2011, para 46, accessible via: https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2011)003rev-e, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

Conclusion

If we return to Fuller[144], the features of law, which he perceives as foundations of the internal morality of law, are not an all-or-nothing affair. On the contrary, they are qualities, which the law and legal systems should aspire to. This implies that the rule of law can, in fact, be considered a matter of degree (Dworkin, p. 5).[145] The level of foreseeability of law can differ and, as showed in the discussed judgement, it certainly does. The CJEU noted that the law which permits the use of coercive powers must itself define the scope of the limitation of the fundamental rights, which it entails. At the same time, in view of the Court, this does not preclude that limitation "from being formulated in terms which are sufficiently open to be able to adapt to different scenarios and keep pace with changing circumstances" (para 114). This openness and flexibility are worrisome. They lower the level of foreseeability and thereby the rule of law's protections. The lower the level of foreseeability, the more pertinent becomes the question how far such law falls short of the ideal of the rule of law, and what marks the point where it can no longer be considered compliant.

[144] Fuller, The Morality of Law (Yale University Press 1969).

[145] See Dworkin's keynote speech in the report on the Venice Commission's Conference on 'The rule of law as a practical concept', p. 5, accessible via: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL%282013%29016-e, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

Challenging Bias and Discrimination in Automated Border Decisions

Evelien Brouwer

In cases where decisions are based on pre-determined criteria or the use of artificial intelligence or AI, it can be difficult to understand not only which risk models or data are used, but also how this use shapes the outcome of the decision-making process. Whereas this ‘black box’ of automated decision making may already have an impact to the right to effective remedies, the possibility to challenge bias or discriminatory criteria in these decisions can be even more difficult.[146] In Algorithmic Discrimination in Europe, Gerards and Xenidis highlight the difficulties to detect and challenge these forms of algorithmic decision-making, amongst others because of the impossibility for judges to get access to information on whether the algorithms or risk models are discriminatory.[147] A particular problem of AI-based risk assessments is the use of apparently ‘neutral’ criteria, which in themselves result in discriminatory decision-making. Only recently, the Dutch Data Protection Authority questioned the proportionality and possible discriminatory use of algorithms and profiling in the short term visa decision-making by the Dutch Ministry of Foreign Affairs.[148]

In *Ligue des droits humains*[149], the Court of Justice of the European Union (CJEU) explicitly addresses the fact that the use of AI and self-learning risk models may deprive data subjects of their right to effective judicial protection as enshrined in Article 47 of the Charter (para. 195). Referring to AG Pitruzzella’s opinion, the CJEU notes that given the opacity which characterises the way in which artificial intelligence technology works, it might be impossible to understand the reason why a given program arrived at a positive match. The CJEU also underlines the problem of challenging algorithmic discrimination, referring to Recital 28 of the Passenger Name Record (PNR) Directive[150], according to which the Directive seeks to ensure

[146] Fundamental Rights Agency, Bias in Algorithms. Artificial Intelligence and Discrimination 2022, p. 50, accessible via: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2022-bias-in-algorithms_en.pdf, last accessed: 26 June 2023.

[147] European Commission, Directorate-General for Justice and Consumers, Gerards, Xenidis, Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination in Europe, 2021, https://op.europa.eu/en/publication-detail/-/publication/082f1dbc-821d-11eb-9ac9-01aa75ed71a1, last accessed: 26 June 2023.

[148] See https://www.nrc.nl/nieuws/2023/05/01/minister-moet-uitleg-geven-over-algoritme-voor-visa-a4163510, last accessed: 26 June 2023.

[149] CJEU, Case C-817/19 *Ligue des droits humains* [21 June 2022].

[150] Directive (EU) 2016/681, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0681, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

'a high level of protection, in particular in order to challenge the non-discriminatory nature of the results obtained'.

The considerations on the right to judicial redress and their meaning for the role of national judiciaries are particularly interesting because of the references made by the CJEU to its earlier case law dealing with immigration law. The importance of this judgment cannot be understated for non-EU citizens.

Direct and indirect discrimination

The right to non-discrimination is protected in Article 14 ECHR and Article 21(1) of the Charter of Fundamental Rights of the European Union (hereafter Charter'). Both provisions include an open-ended formulation of grounds for exclusion, such as sex, ethnicity, religion, or political belief. However, the use of apparently 'neutral' factors may also lead to prohibited discrimination within the meaning of Article 14 of the ECHR.[151] Where such 'neutral' criteria can place individuals belonging to a minority group in a disadvantaged situation, this may result in an indirect form of discrimination. The Dutch child benefits scandal illustrated how the use of an automated pre-risk assessment by the tax authorities, based on criteria such as the fact whether or not a person had a double nationality, or supposedly neutral characteristics such as the postal code of someone's home, could result in a both direct and indirect discriminatory selection.[152] Furthermore, a legal distinction based on nationality (or, as in this case, the length of time a person has a nationality) could result in prohibited discrimination, if such policy has a racial basis, making it an indirect distinction based on race or ethnicity.[153] The intentions of acting persons or bodies are not the only criteria: even without discriminatory intentions, the acts may nonetheless be illegally discriminatory. Without objective and reasonable justification, measures with disproportionate and prejudiced effects on a specific group are prohibited.[154]

The right to non-discrimination is incorporated in the PNR Directive. Article 6(4) of the PNR Directive provides that any assessment of travelers prior to their arrival against pre-determined criteria must be carried out in a non-discriminatory manner: this means, according to the CJEU,

[151] See ECtHR, *D.H. v. Czech Republic* App no 57325/00 [13 November 2007].

[152] See ten Seldam/Brenninkmeijer, The Dutch benefits scandal: a cautionary tale for algorithmic enforcement, EU Law Enforcement, 30 April 2021, accesible via: https://eulawenforcement.com/?p=7941, last accessed: 26 June 2023.

[153] ECtHR, *Biao v. Denmark* App no 38590/10 [24 May 2016], para 114.

[154] ECtHR, *Biao v. Denmark* App no 38590/10 [24 May 2016], para 92.

Electronic copy available at: https://ssrn.com/abstract=4547775

that this provision covers both direct and indirect discrimination. In order to protect the non-discriminatory and proportional use of pre-determined criteria, the CJEU defines four conditions (paras 197-201). First, to avoid direct and indirect discrimination, these criteria must be defined in such a way that ‘while worded in a neutral fashion, their application does not place persons having the protected characteristics at a particular disadvantage.’ For this purpose, PIU’s should establish in a ‘clear and precise manner, objective review criteria’. Second, to ensure the targeted, proportionate and specific nature of the pre-determined criteria, they must target specifical individuals who ‘might be reasonably suspected of involvement in terrorist offences or serious crime’ as covered by the PNR Directive. Third, in order to contribute to the reliability and proportionality of (the use of) those criteria, they must take consideration of both the incriminating and exonerating circumstances involved. Last, following the strict necessity test, the pre-determined criteria must be reviewed regularly. This latter requirement means, according to the CJEU, that the criteria must be updated in accordance with the circumstances justifying their being taken in to consideration, but also taking into account acquired experience to reduce the number of ‘false positives’ as much as possible. The CJEU underlines the role of national PIUs to ensure the implementation of these safeguards by referring to Article 6(5) and (6) of the Directive. They should individually review any positive match by non-automated means in order to identify ‘as much as possible’ any ‘false positives’, but also to exclude any discriminatory results (para. 203). While the CJEU emphasizes as such the responsibility of Member States to ensure a non-discriminatory risk assessment, it at the same time offers wide discretionary power to decide on what should be considered as a ‘clear and precise’ formulation of ‘objective review criteria’. Here, the chosen formula of ‘acquired experience’ does not provide a guarantee for excluding any personal bias in the decision-making of PIU officers. This leaves an important but also difficult role for courts to detect and prove discrimination.

Right to effective judicial protection

The right to judicial redress is included in Article 13 (1) of the PNR Directive. This provides that in respect to all processing of personal data pursuant to this Directive, every passenger shall have the same right to protection of their personal data, rights of access, rectification, erasure and restriction, as well as the rights to compensation and judicial redress as laid down in EU and national law, and in the implementation of the Framework Decision 2009/977 (now

Electronic copy available at: https://ssrn.com/abstract=4547775

replaced by the Law Enforcement Directive or 'LED'[155]). Importantly, in *Ligue des droits humains*, the CJEU emphasizes the necessity of transparent and informed decision-making, not only for the right to judicial redress itself, but also to allow the individual to decide whether or not to lodge an appeal.

According to the CJEU, this safeguard is particularly necessary in cases where AI based decision-making includes the risk of discriminatory outcomes. In general, the CJEU follows the AG in the conclusion that the PNR Directive precludes the use of artificial intelligence in self-learning systems or in 'machine-learning' capable of modifying the assessment process without human intervention or review. This ban applies, as explained further by Gerards in her contribution to this Verfassungsblog series, to the development of assessment criteria to be used in the screening process, including the weighing of those criteria (para. 194). Importantly, the CJEU considers that the use of such technology makes it impossible for data subjects to understand the reason why a given program arrives at a positive match and to challenge the non-discriminatory nature of the results. This problem, according to the CJEU, is related to the 'opacity which characterizes the way in which artificial intelligence works', depriving data subjects of their right to effective judicial protection as protected in Article 47 of the Charter (para. 195).

On the basis of Article 13 (1), competent authorities must ensure, according to the CJEU, that the person concerned is able to understand 'how those criteria and those programs work' to allow him or her to decide 'with full knowledge of the relevant facts' whether or not to claim the unlawful and indiscriminatory nature of these criteria (para. 201). For the CJEU, this obligation does not necessarily mean that a person is allowed 'during the administrative procedure, to become aware of the pre-determined assessment criteria' (para. 210). These findings do raise questions on the practical implication of this right to information: how can someone refused to embark on a flight address the possibly discriminatory nature of the prior risk assessment or calculate his or her chances for a successful judicial review without knowing the assessment criteria?

The CJEU seems to be aware of this problem where it refers in *Ligue des droits humains* to earlier case-law dealing with Article 47 of the Charter, in order to clarify the scope of protection under Article 13 (1) of the PNR (paras 210-211). The CJEU mentions two judgments in the

[155] Directive (EU) 2016/681, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0681, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

context of migration: *R.N.N.S. and K.A. v Minister van Buitenlandse Zaken*[156] and *ZZ v. SSHD.*[157] *R.N.N.S. and K.A. v Minister van Buitenlandse Zaken* concerned the right to effective remedies against the refusal of a short-term visa by a Member State on the basis of an objection from another Member State, which had been consulted in accordance with the rules in Articles 22 and 23 of the Visa Code.[158] Generally, in these cases, the visa applicants are not informed about the precise content of the objection, or even by which Member State the objection was raised. These practices may result in a kind of 'black box' decision-making, comparable to the use of algorithms or automated decision-making. It is therefore to be welcomed that the CJEU implicitly draws this parallel, applying procedural guarantees as defined for visa decision-making to the context of the PNR Directive. The CJEU refers to paragraph 43 of the R.N.N.S. judgment, in which it held that in order to ensure that the judicial review guaranteed by Article 47 of the Charter is effective, 'the person concerned must be able to ascertain the reasons upon which the decision taken in relation to him or her is based, either by reading the decision itself or by requesting and obtaining notification of those reasons'.[159] In *R.N.N.S*, the CJEU further clarified that the court with jurisdiction should have the power 'to require the authority concerned to provide that information, so as to make it possible for him or her to defend his or her rights in the best possible conditions and to decide, with full knowledge of the relevant facts, whether there is any point in applying to the court with jurisdiction'.[160] This information should put the national court 'in a position in which it may carry out the review of the lawfulness of the national decision in question.'.[161] The reference by the CJEU in *Ligue des droits humains* to the *R.N.N.S.* ruling is important for two reasons. First, the CJEU obliges Member States to ensure that individuals have access to national courts which are empowered to review the lawfulness of the use of pre-determined criteria and the programs applying them. Second, Member States must also guarantee access to courts which are able to examine all the grounds and evidence on the basis of which PNR decisions were taken. In *R.N.N.S.*, the CJEU also stressed the relevance of the fundamental right to good governance, included in Article 41

[156] CJEU, Cases C-225/19 and 226/19 *R.N.N.S. and K.A. v Minister van Buitenlandse Zaken* [24 November 2020].
[157] CJEU, Case C-300/11 *ZZ v Secretary of State for the Home Department* [4 June 2013].
[158] Regulation (EC) No 810/2009, accessible via: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32009R0810, last accessed: 26 June 2023.
[159] CJEU, Case C-817/19 *Ligue des droits humains* [21 June 2022], para 210.
[160] CJEU, Cases C-225/19 and 226/19 *R.N.N.S. and K.A. v Minister van Buitenlandse Zaken* [24 November 2020], para 43.
[161] CJEU, Cases C-225/19 and 226/19 *R.N.N.S. and K.A. v Minister van Buitenlandse Zaken* [24 November 2020], para 43.

Electronic copy available at: https://ssrn.com/abstract=4547775

of the Charter, obliging national authorities to give reasons for its decisions.[162] Whereas the wording of Article 41 only protects an individual in his or her relation with EU institutions, the CJEU held in *R.N.N.S.*, as already stated in previous cases[163], that the right to good administration reflects a general principle of EU law which is applicable to Member States when they are implementing that law, to the effect that this encompasses the obligation of the administration to give reasons for its decisions.[164]

Furthermore, in *Ligue des droits humains*, the CJEU underlines that not only a court, responsible for reviewing the legality of the decision adopted by the competent authorities, but also the individual must have the opportunity to examine 'all the grounds and the evidence on the basis of which the decision was taken' (para. 211). In cases of AI-based decision-making, not having access to all the grounds or evidence is exactly the problem. Interestingly, the CJEU refers at this point to its judgment in the *ZZ* case. In this case concerning the expulsion of a EU citizen on the basis of national security grounds, the CJEU held that 'having regard to the adversarial principle that forms part of the rights of the defence, which are referred to in Article 47 of the Charter, the parties to a case must have the right to examine all the documents or observations submitted to the court for the purpose of influencing its decision, and to comment on them'.[165] According to the CJEU, the fundamental right to an effective legal remedy would be infringed, if a judicial decision were founded on facts and documents which the parties themselves, or one of them, have not had an opportunity to examine and on which they have therefore been unable to state their views.[166] Where a Member State invokes reasons of state security, a competent national authority must be entrusted to verify and be able to carry out an independent examination whether those reasons 'stand in the way of precise and full disclosure of the grounds on which the decision in question is based and of the related evidence'.[167] It is for the Member State to prove, in accordance with the national procedural rules, that State security would in fact be compromised by 'precise and full disclosure to the person concerned'.[168]

[162] CJEU, Cases C-225/19 and 226/19 *R.N.N.S. and K.A. v Minister van Buitenlandse Zaken* [24 November 2020], para 33.

[163] See for example CJEU Cases C-141/12 and 372/12 *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S* [17 July 2014].

[164] CJEU, Cases C-225/19 and 226/19 *R.N.N.S. and K.A. v Minister van Buitenlandse Zaken* [24 November 2020], para 34.

[165] CJEU, Case C-300/11 *ZZ v Secretary of State for the Home Department* [4 June 2013], para 55.

[166] CJEU, Case C-300/11 *ZZ v Secretary of State for the Home Department* [4 June 2013], para 56.

[167] CJEU, Case C-300/11 *ZZ v Secretary of State for the Home Department* [4 June 2013], paras 60-62.

[168] CJEU, Case C-300/11 *ZZ v Secretary of State for the Home Department* [4 June 2013], paras 61-62.

Electronic copy available at: https://ssrn.com/abstract=4547775

Of course, the right to legal redress vis-à-vis individual decisions should be read complementarily to the right to legal remedies with regard to the data protection rights in general. This right, as developed by the CJEU in amongst others Opinion 1/15[169], *Quadrature du Net*[170], or *Smaranda Bara and Others*[171] remains relevant in the context of data processing on the basis of the PNR Directive, including the use of data for pre-risk assessment.

Conclusion

As explained elsewhere[172], the involvement of different Member States and actors in the decision-making on who is allowed entrance and who is not already makes it difficult for non-EU citizens to challenge border decisions. The flagging of persons who are identified as security risks during AI-based risk assessments will cause an additional barrier, not only for the mobility of persons, but also for the protection of their individual rights. This judgment, in which the CJEU emphasizes the necessity of effective judicial protection, is therefore of particular importance for non-EU citizens, who are increasingly confronted with the use of automated border decisions, on the basis of the use of large-scale databases and risk assessments, as for example provided in the more recent ETIAS Regulation. While the PNR Directive and the ETIAS Regulation[173], as has been highlighted in the report Artificial Intelligence at EU borders[174], prohibit the use of criteria which entail a high risk of discrimination for risk indicators (ethnicity, race, religious beliefs), these characteristics can also be correlated with or inferred from other types of data. This may result in (prohibited) indirect discrimination. In practice, it will remain difficult for both individuals and courts to detect and prove the discriminatory nature of these decisions. For this problem, the question whether any bias exists in the automated risk model or the 'acquired experience' of the individual PIU officer, does not seem to make much difference. Nevertheless, it is to be welcomed that the CJEU defines procedural safeguards for both the individual as the judiciary to ensure the right to effective judicial protection in AI based decision-making, also to

[169] CJEU, Opinion 1/15 of the Court [26 July 2017].

[170] CJEU, Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net* [6 October 2020].

[171] CJEU, Case 201/14 *Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate et al.* [1 October 2015].

[172] Brouwer, Schengen and the Administration of Exclusion: Legal Remedies Caught in between Entry Bans, Risk Assessment and Artificial Intelligence, (2021) 23 European Journal of Migration and Law, 485.

[173] Regulation (EU) 2018/1240, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1240, last accessed: 26 June 2023.

[174] European Parliamentary Research Service, Dumbrava, Artificial intelligence at EU borders, July 2021, https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

challenge discrimination. Whereas the importance of this judgment certainly reaches beyond immigration and border policies, the relevance for non-EU citizens should not be overlooked.

Electronic copy available at: https://ssrn.com/abstract=4547775

EU Privacy and Public-Private Collaboration

Chloé Berthélémy

Ligue des Droits Humains and Private Standard-Setting

A widely noted international trend is the delegation of core state functions, such as law enforcement, to private actors.[175] Nowhere is this more apparent than in the development and use of security technologies. For instance, police authorities increasingly use Artificial Intelligence (AI) tools created and managed by the private sector – claims of efficiency, speed and accuracy justify their use. This public-private collaboration harbours detrimental consequences for fundamental rights and the rule of law, in particular, the principle of legality.

In this blog, I focus on three different categories of private actors' participation in the European Union's (EU) security policy arena. I illustrate this through a number of policy examples on coerced, voluntary and proactive forms of "cooperation" between the public and private sector, and their effects on the rule of law. The policy outcomes which result from this public-private collaboration are not democratically accountable, and allow human rights to be superseded by private, profit-driven interests.

Legal obligations

The standard situation of public-private cooperation is one of state regulation requiring private sector compliance. In this scenario, private actors react to the legal norms imposed on them. In the context of Passenger Name Record (PNR) data, this occurred already in the 1990s in the USA, when US authorities required airline carriers to provide personal (PNR) data on travellers for security purposes.[176] After 2001, the USA's insistence on the transfer of PNR data proliferated globally, and the first controversies regarding the protection of personal data and its transfer to foreign states (i.e., the USA) emerged.[177] The transfer of personal data by companies operating in the EU to a foreign country, where EU data protection rules would not

[175] See Abrahamsen/Leander (eds), Routledge Handbook of Private Security Studies (Routledge 2016).
[176] See Argomaniz, When the EU is the 'Norm-taker': The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms, (2009) 31 European Integration, 119; see also in this volume: Bigo/Salomon, Passenger Name Records and Security.
[177] Brouwer, The EU Passenger Name Record (PNR) System and Human Rights, CEPS Working Document No. 320/September 2009, accessible via: http://aei.pitt.edu/11485/1/1903.pdf, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

apply, was at the heart of this debate.[178] Despite early controversy, the EU's tendency to mimic US approaches in some areas of securitisation is particularly apparent here. By 2016, the EU had adopted legislation requiring the transfer of PNR data by carriers to destination authorities, covering both flights into and out of the EU, as well as intra-EU ones (although the latter was not mandatory).[179] The resulting controversy is the subject of this broader blog series, while the resulting impacts on fundamental rights are discussed in the third section of this blog.

The harnessing of the private sector in achieving security goals is also apparent in the area of online content governance and surveillance. The Regulation on Disseminating Terrorist Content Online, adopted in 2021[180], and the proposed Child Sexual Abuse Regulation (CSAR)[181] showcase how EU legislation furthers a form of securitisation of the internet.[182] The objective is no longer to regulate the conduct of business as such but rather to pursue law enforcement purposes and security policy goals. The consequence is the integration of internet platforms into state security activities as central actors. For example, it is clear that, although the CSAR is lex specialis to the Digital Services Act[183] – the EU's core legislative piece for regulating illegal content on intermediaries – and its legal basis is Article 114 of the Treaty on the Functioning of the European Union, which supports harmonising measures for the internal market, other parts of the CSAR clearly relate to the practices of law enforcement. The absence of a legal basis for law enforcement competencies in the EU, introduced instead under the cover of internet regulation, enables a harmful privatisation of the protection of children, which is and should remain a law enforcement responsibility.

Private standard-setting

The problem of achieving law enforcement and security goals by way of internet regulation is further exacerbated by the promotion and adoption of privately-developed standards and

[178] Kuskonmaz/Guild, EU exclusive jurisdiction on surveillance related to terrorism and serious transnational crime, case review on opinion 1/15 of the CJEU, (2018) 43 European Law Review, 583.
[179] Directive (EU) 2016/681, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0681, last accessed: 26 June 2023.
[180] Regulation (EU) 2021/784, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32021R0784, last accessed: 26 June 2023.
[181] Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0209, last accessed: 26 June 2023.
[182] Deibert/Rohozinski in: Deibert/Palfrey/Rohozinski/Zittrain/Stein (eds), Access Denied: The Practice and Policy of Global Internet Filtering (MIT Press 2008), 123.
[183] Regulation (EU) 2022/2065, accessible via: https://eur-lex.europa.eu/eli/reg/2022/2065/oj, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

practices as implementation norms. The reasoning behind this endorsement of private actors' standards in digital policies is that they are better placed than the legislator to know what is efficient and realistically achievable. In the content governance field, this often takes place through the prescribed deployment of risk assessment tools and proactive measures, a strategy of incentivizing certain outcomes while leaving it to the private sector to define how to reach them. Although the reasoning of state actors in drawing on the private sector is the desire to build on industry best practices, the outcomes are the use of so-called technology-neutral tools, which are too controversial for the public sector, and constitute blatant challenges to key principles of EU data protection and internet regulation.

For example, the use of content automatic filters (also known as 'upload filters') and hash databases that monitor, identify and remove content have already been put in place by social media platforms. These tools have been promoted as the industry-wide solution in the fight against terrorist content and online radicalisation – an apparent simple answer to a very complex societal issue. However, it has been repeatedly demonstrated how these tools fail to assess the context of publications accurately, thus leading to the worrying censorship of legitimate expression.[184] They also constitute a form of mass monitoring, contradicting the EU's own legal values.

In the context of the ongoing negotiations on the CSAR proposal, a (dominant) part of the technology industry is attempting to seize the opportunity of the proposed series of new user surveillance obligations by suggesting their technological products as solutions, and having the legislation impose them on their competitors.[185] One of them, extremely controversial, is called "client-side scanning", an intrusive technology that circumvents end-to-end encryption.[186] This shows that depending on their position on the market, private actors either put up with legal obligations and try to adapt, or they exploit them to cement their dominance by seeking new market opportunities and making their products the legal standard (further discussed in the last part of this blogpost).

[184] Pirkova, Automation and illegal content: can we rely on machines making decisions for us?, Access Now, 17 February 2020, https://www.accessnow.org/automation-and-illegal-content-can-we-rely-on-machines-making-decisions-for-us/, last accessed: 26 June 2023.

[185] Netzpolitik, How a Hollywood star lobbies the EU for more surveillance, EDRI, 25 May 2022, https://edri.org/our-work/how-a-hollywood-star-lobbies-the-eu-for-more-surveillance/, last accessed: 26 June 2023.

[186] For an explanation of the concept see Abelson et al., Bugs in our Pockets: The Risks of Client-Side Scanning, arxiv.org, 14 October 2021, accessible via: https://arxiv.org/abs/2110.07450, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

The PNR Directive placed private actors in the air transport sector in a complicated position. While some airlines collect PNR data as part of their commercial practices to improve services to regular customers, not all airlines do so directly. The obligation to transfer this data to public sector actors in countries other than the one where the data was collected (mainly the USA, Canada and Australia) meant that many companies chose to outsource the collection and transfer to other companies specialising in this service.[187] The private sector itself did not challenge the legislation requiring it to provide access to this personal data. It acquiesced to state demands but insisted that inter-state agreements were entered into, to protect private sector actors from challenges by individuals.[188] Instead, the legal challenges in the EU context were launched by the European Parliament[189] and, more recently, by specialised NGOs[190].

Voluntary Disclosure

Another form of private sector involvement as regards public sector demands on access to personal data for law enforcement purposes (notably in criminal investigations) is 'voluntary cooperation'. Private actors are encouraged to disclose their clients' personal data 'informally', outside the scope of the law. Europol's 2022 SIRIUS EU Digital Evidence Situation Report[191] reveals that direct requests for data to foreign-based online service providers under 'voluntary cooperation' continue to be widely used in the EU. 63% of officers indicated direct requests as their main type of request in 2021, whereas only 19% favour legal judicial cooperation channels.

This approach, which is much favoured by public authorities, side steps the problem of fundamental rights and data protection. Indeed, voluntary data disclosure represents further processing of that data by the private controller for a purpose inconsistent with the original purpose – which is expressly prohibited under the General Data Protection Regulation (GDPR). Nevertheless, the practice shows that data controllers, rather than looking to their obligations in EU law, frequently merely acquiesce as the requests are coming from state authorities, so

[187] See Zureik/Salter, Global Surveillance and Policing (Routledge 2005).

[188] Yano, Come the (Unfriendly?) Skies: Negotiating Passenger Name Record Agreements Between the United States and European Union, (2010) 5 Journal of Law and Policy for the Information Society, 479.

[189] See Tambou, Opinion 1/15 on the EU-Canada Passenger Name Record (PNR) Agreement: PNR Agreements Need to Be Compatible with EU Fundamental Rights, (2018) 23 European Foreign Affairs Review, 187.

[190] This was the case in *Ligue des droits humains*, CJEU, Case C-817/19 *Ligue des droits humains* [21 June 2022].

[191] Accessible via: https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_DESR_2022.pdf, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

voluntary cooperation is assumed to be lawful. To the contrary – data disclosure to law enforcement bodies should always be regarded as a restriction of fundamental rights that must be provided for by law and satisfy requirements of necessity and proportionality in accordance with Article 52(1) of the Charter.

Despite the blatant legal uncertainty of this practice, EU legislation demonstrates a trend of voluntary disclosure of personal data by the private sector outside any legal basis. In the recent reform of Europol's mandate[192], private actors are strongly incentivised to breach personal data protection rules by 'cooperating' with Europol. This only creates extensive problems around transparency and accountability, while at the same time undermining fundamental rights, in particular, procedural rights.

The question of lawfulness is very much known by the institutions themselves. Europol's Data Protection Function (DPF) was consulted to assess compliance of the practice with data protection law.[193] To date, there are no final conclusions from the various data protection authorities involved in this process on this question.

A feedback loop between financial support and legislative agenda-setting

Another reaction of the private sector has been to proactively engage with public sector law enforcement (or other agencies) to take control of the policy-making agenda and to jointly shape policies in directions which are beneficial to the private sector itself. In the security field, technological development usually precedes the establishment of a legal basis. The industry develops security solutions to sell to state authorities and, at worst, they do so by receiving EU public funds. Once the system is already in place, it's like a fait accompli. The only thing missing is legal backing.

For example, the development of national PNR systems were helped along with at least €50 million by the Commission, years before an EU Directive was finally agreed upon in April 2016.[194] The Eurosur border surveillance system was in development for at least five years

[192] See Regulation (EU) 2022/991, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.169.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A169%3ATOC, last accessed: 26 June 2023.

[193] See the Annual Report of the Data Protection Officer 2021, accessible via: https://www.europol.europa.eu/cms/sites/default/files/documents/EDOC%20-%231275369-v1-Public%20version%20of%20EDOC-%231196888-v10-DPO_Annual_Report_2021_Redacted.PDF, last accessed: 26 June 2023.

[194] See Statewatch, Commission makes €50 million available for the development of "big brother" PNR databases - before legislation has even been agreed, 28 March 2012, accessible via:

Electronic copy available at: https://ssrn.com/abstract=4547775

before legislation was approved in 2013, with numerous EU research projects helping put the pieces in place before a Portuguese firm won the multi-million-euro maintenance contract. The 'smart borders' project involving the Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS) followed a similar path – research projects helped develop the technology in the last decade, but the complementary legislation only came up for adoption years later, while the implementation deadline has been postponed several times by now.

In terms of agenda-setting, the International Civil Aviation Organisation (ICAO), a specialised agency of the United Nations that coordinates the principles and techniques of air travel, is being used as a forum for policy influence by both governments and the travel industry to promote "worldwide tracking, surveillance, and control of all individuals' movements.".[195] Airlines are active participants in ICAO working groups and use them to impose their own technical standards for PNR data collection and storage. By governing the data collection processes, they minimise their burden of collecting additional data, selecting or reformatting passenger data differently, to satisfy different governments' demands. That way they become norm-setters.

Lastly, Statewatch's report on 'the development of the EU security-industrial complex' shows through the example of "the legislative procedure that led to the establishment of the €1.7 billion security research programme within Horizon 2020" how different corporate interests engage in the design and implementation of the EU security policy, literally co-drafting the legislation along with the EU institutions.[196]

Consequences

The consequences for fundamental rights and the rule of law are enormous. At the most basic, private agenda- and technical standard-setting constitutes corporate capture of the legislative agenda and process, which should be democratic and not guided by profit-driven interests. The

https://www.statewatch.org/news/2013/january/statewatch-news-online-eu-commission-makes-128-50-million-available-for-the-development-of-quot-big-brother-quot-pnr-databases-before-legislation-has-even-been-agreed/, last accessed: 26 June 2023.

[195] Hasbrouck, ICAO mandates worldwide government surveillance of air travelers, EDRI, 10 September 2020, https://edri.org/our-work/icao-mandates-worldwide-government-surveillance-of-air-travelers/, last accessed: 23 June 2023.

[196] Jones, Market Forces – The Development oft he EU Security-Industrial Complex, Statewatch 2020, accessible via: https://www.statewatch.org/media/documents/analyses/marketforces.pdf, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

extensive use of EU funds transferred to the private sector through security research programmes represents a grave diversion of public resources towards harmful tech applications and uses.

In all three public-private collaboration cases presented in this blog, the risk is that human rights are superseded by security objectives. The public-private security community sketched out above, that bridges corporate interests and government policy, while benefiting from a disturbing lack of democratic accountability, should be urgently called into question.

Electronic copy available at: https://ssrn.com/abstract=4547775

Squaring the triangle of fundamental rights concerns

Daniel Mügge

The CJEU's PNR ruling and AI governance

Ex ante, the July 2022 ruling by the Court of Justice of the EU (CJEU) on Passenger Name Records (PNR)[197] had a very specific scope — the use of passenger name records by government agencies. Upon closer inspection, however, it has important implications for the governance of algorithms more generally. That is true especially for the proposed AI Act[198], which is currently working its way through the EU institutions. It highlights, ultimately, how national, or in this case European, legal orders may limit the scope for international regulatory harmonization and cooperation.

A potential clash with jurisprudential limits on AI policies

First of all, the PNR ruling, and the changes to the PNR Directive[199] it implies, are a simple reminder that EU legislation is open to challenge in court. Obvious as it may seem, this consideration has hardly figured in debates about the AI Act. A wide range of stakeholders — including NGOs but also EU bodies such as the European Data Protection Supervisor—have voiced concerns about AI regulation plans. Those concerns frequently revolved around potential violations of ethical norms, for example, the right to privacy or non-discrimination. Most of these standpoints combined ethical arguments about what is desirable or not with technological arguments about the actual effects the application of certain algorithms would have. In contrast, few arguments considered whether certain AI use cases would even withstand legal scrutiny by the CJEU because they might violate fundamental rights, as outlined below.

This silence is remarkable. Many experts genuinely puzzle over when and where algorithms and fundamental rights may clash. And not only are there no easy answers: because of the speed with which AI technologies evolve, it is easily conceivable that legally contentious use cases emerge for which present-day law, and also a future AI Act, had not provided. (The haste with which provisions about generative AI were inserted into the negotiations at the 11th

[197] CJEU, Case C-817/19 *Ligue des droits humains* [21 June 2022].

[198] COM/2021/206 final, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206, last accessed: 26 June 2023.

[199] Directive (EU) 2016/681, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0681, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

hour[200] is instructive.) Sooner or later, legal challenges to the AI Act are to be expected, and it is anybody's guess how those will look, and how they will be decided.

The PNR ruling points to additional complications: one common discussion topic in AI debates is the explainability of algorithmic output, especially when algorithms are used in public policy decisions affecting individuals. Worries about discrimination also feature widely. At least with respect to the use of PNR in law enforcement and security contexts, however, the CJEU puts the bar even higher: the PNR Directive itself requires that criteria for identifying subjects have to be "pre-determined" (§6.2(b)), and the Court finds that to be incompatible with self-learning algorithms as long as the output is not transparent to humans.[201] It thus turns the PNR Directive's own wording against the use of algorithmic tools.

At the same time, in paragraph 195 of its ruling, it cites Article 47 of the EU Charter of Fundamental Rights — the right to an effective remedy — as potentially at odds with opaque and implicit selection criteria. This interpretation suggests that "unexplainable AI" might face much broader limitations in its applicability than only emanating from, in this case, the PNR Directive itself. After all, algorithms' added value is to identify patterns in the data that humans would miss — self-learning algorithms are used precisely where criterium pre-definition fails. That may spell broader trouble for their use in public policy when potential fundamental rights are on the line.

Moreover, the ruling underlined the importance of proportionality: may potential rights-infringements be justified in light of the security risks that they tackle? Again, this question is thorny, because the potential uses of AI vary highly in the level of risks that they claim to address. Blanket rules for or against employing potentially rights-infringing AI in law enforcement seem difficult from that angle.

Irrespective of where one stands on these issues, the key is that there is significant scope for legal challenges of provisions in the AI Act. As the Schrems cases as well as the PNR ruling have shown, these kinds of challenges may be successful and can have momentous consequences. Up to now, there seems to be little realization that any compromises coming out

[200] Bertuzzi, Leading EU lawmakers propose obligatoins for General Purpose AI, EURACTIV, 14 March 2023, https://www.euractiv.com/section/artificial-intelligence/news/leading-eu-lawmakers-propose-obligations-for-general-purpose-ai/, last accessed: 26 June 2023.

[201] Thönnes, A Directive altered beyond recognition, Verfassungsblog, 23 June 2022, https://verfassungsblog.de/pnr-recognition/, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

of the AI Act trilogues might, at least in part, not withstand legal scrutiny, either now or in the future.

Extraterritorial implications

While a future AI regime for Europe is being negotiated, EU representatives have also been heavily involved in international talks and exchanges to craft AI rules. Those concern especially the OECD, whose official AI definition from 2019[202] recently emerged as a proposed compromise for the EU's own legislation[203], and the Trade and Technology Council, the forum for transatlantic policy exchange and negotiation, which largely concentrates on digital technologies. Alignment of EU policy with international rules, and their embedding in a sort of transatlantic regulatory regime, are both important European policy goals. What does the PNR ruling imply for such efforts?

To begin, one reading of the CJEU's decision is that, at least for certain use cases, EU citizens' right to effective judicial remedies as spelled out in Article 47 of the EU Charter of Fundamental Rights is incompatible with algorithms whose results cannot be translated into clear criteria and are not certified discrimination-free. If so, that would generate hard limits on the AI-powered services and applications which non-EU companies could offer in the EU, either directly or indirectly. The AI Act may impose such limits on its own, as well. As an implication of the PNR ruling, or its juridical spirit, these limits would swing free from the will of legislators. In other words, the fundamental rights of EU citizens, as interpreted by the CJEU, may define the outer boundaries of regulatory cooperation in the AI field — no matter how much goodwill there might be to find a compromise with, for example, the USA. Irrespective of whether these limits would be heeded in transatlantic or multilateral negotiations ex ante, or would emerge later on through successful legal challenges, as happened in the Schrems cases, they might cause serious frustrations among the EU's international partners.

This logic also casts its shadow on the outsourcing of rule-making to technocratic expert bodies, such as the European Committee for Standardization and the European Electrotechnical

[202] See OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449, 22 May 2019, accessible via: https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449, last accessed: 26 June 2023.
[203] Bertuzzi, EU lawmakers set to settle on OECD definition for Artificial Intelligence, EURACTIV, 7 March 2023, https://www.euractiv.com/section/artificial-intelligence/news/eu-lawmakers-set-to-settle-on-oecd-definition-for-artificial-intelligence/, last accessed: 26 June 2023.

Electronic copy available at: https://ssrn.com/abstract=4547775

Committee for Standardization[204], and potentially the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as their global counterparts. Already, the relevant global standard setting committees (subcommittee 42 of the ISO/IEC[205]) ponder to what degree they would or should enter political or normative territory with their efforts, for example, to devise procedures to determine algorithmic bias. On the one hand, the CJEU's own interpretation of what would constitute a legally robust definition of such thorny concepts might compromise the formal independence of technical standard setters, given that fundamental rights would take precedence over any "technical" compromise the latter might devise. On the other hand, if such compromises were found to withstand legal scrutiny, they might offer an escape from otherwise fraught legal and ethical debates. Either way, the scope for outsourcing standard definitions that touch on fundamental rights questions would itself depend on the view of, and potential review by, the CJEU.

Finally, many aspects of AI technologies and their applications are bound to evolve significantly in the future. That includes the kind of data available to train them, technological ways to extract comprehensible "criteria" for (suggested) decisions from algorithms, and forms of applying them. As is the case generally, the legal framework for AI will therefore have to be dynamic in order to accommodate future technological and societal developments. This, too, limits the degree to which legislators or negotiators could lock the EU into particular bilateral or multilateral agreements on AI governance.

Future scenarios

If the PNR ruling implies that fundamental rights of EU citizens may demarcate the outer limits of EU-external regulatory cooperation, which scenarios does that suggest for the future? One scenario, somewhat surprisingly, is a form of inadvertent Brussels effect — but very different from Bradford's original logic[206] (Bradford 2020). Here, other parties to regulatory negotiations might appreciate, however grudgingly, that certain safeguards in EU law may be unavoidable, no matter what they think of them — once more, the Schrems cases are instructive. The EU's limited room for manoeuvre on some of these questions may, in fact, strengthen its bargaining position.

[204] Veale/Borgesius, Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach, (2021) 22 Computer Law Review International, 97.
[205] See https://www.iso.org/committee/6794475.html, last accessed: 26 June 2023.
[206] Bradford, The Brussels Effect: How the European Union Rules the World (Columbia Law School 2020).

Electronic copy available at: https://ssrn.com/abstract=4547775

It is equally plausible, however, that divergent regulatory preferences and unwillingness, or inability, to compromise might generate disparate levels of regulatory stringency even among, for example, the USA and the EU. If so, companies might "level up" to presumably higher EU standards voluntarily in the products they offer — a dynamic that David Vogel (1995) has dubbed the California effect[207], in which American car producers voluntarily embraced stringent Californian environmental rules across their product palette. Alternatively, markets for AI-powered products might fragment to some degree, with more or less different versions of products on offer in different jurisdictions, each compliant with local laws. And, depending on how difficult it is to custom-tailor products to diverse regulatory regimes, some companies might opt to forego EU market access altogether, even if its overall market size is likely to mitigate against that approach.

In the meantime, the geopolitical climate has continued to deteriorate, not only in light of the Russian war against Ukraine, but also through souring Sino-American relations. AI governance, not least in the EU itself, had initially largely been framed as a technological, commercial and societal issue. Certainly, since the publication of the report by the American National Security Commission on Artificial Intelligence[208], however, AI technologies are increasingly viewed through a security and military lens.[209] The EU AI Act itself steers clear of the intersection between AI and national security, not least in light of the EU's limited competences there. To the degree that more and more aspects of AI governance were to be framed as security-relevant — for example, because of AI technologies' dual use character — the scope of the AI Act provisions and the protections they provide might shrink. It will be interesting to see whether the CJEU, and its interpretation of fundamental rights, will then fill that gap and provide guardrails for AI development and application that at present are hardly considered.

[207] Vogel, Trading up : consumer and environmental regulation in a global economy (Harvard University Press 1995).

[208] NSAI, Final Report, 2021, accessible via: https://www.nscai.gov/2021-final-report/, last accessed: 26 June 2023.

[209] Mügge, The securitization oft he EU's digital tech regulation, (2023) 30 Journal of European Public Policy, 1431.

Electronic copy available at: https://ssrn.com/abstract=4547775

The dilemma of fundamental rights, the need for legal flexibility, and international agreements

Taken together, algorithms may constitute a fundamental rights governance challenge, squeezing from three sides: first, fundamental rights as interpreted by the CJEU impose hard limits on what is and is not permissible. Second, at the same time, the speedy development of the technologies themselves would seem to call for a much more open-ended and flexible legal framework. And third, geopolitical as well as economic imperatives would seem to require the ability to commit to international agreements, irrespective of the former two considerations. The PNR ruling suggests how difficult that triangle will be to square, not only for passenger data, but for algorithms more generally.

Electronic copy available at: https://ssrn.com/abstract=4547775