frontiers | Frontiers in Political Science

TYPE Policy and Practice Reviews
PUBLISHED 16 October 2023
DOI 10.3389/fpos.2023.1232601

OPEN ACCESS

EDITED BY
Monika Zalnieriute,
University of New South Wales, Australia

REVIEWED BY
Nicola Lettieri,
Istituto Nazionale per l'Analisi delle Politiche Pubbliche (INAPP), Italy
Niovi Vavoula,
Queen Mary University of London, United Kingdom
Tommaso Venturini,
Centre Internet et Société (CNRS), France

*CORRESPONDENCE
Lucas Michael Haitsma
✉ l.m.haitsma@rug.nl

RECEIVED 31 May 2023
ACCEPTED 19 September 2023
PUBLISHED 16 October 2023

CITATION
Haitsma LM (2023) Regulating algorithmic discrimination through adjudication: the Court of Justice of the European Union on discrimination in algorithmic profiling based on PNR data. *Front. Polit. Sci.* 5:1232601. doi: 10.3389/fpos.2023.1232601

Regulating algorithmic discrimination through adjudication: the Court of Justice of the European Union on discrimination in algorithmic profiling based on PNR data

Lucas Michael Haitsma*

Department of Constitutional Law, Administrative Law and Public Administration, Faculty of Law, University of Groningen, Groningen, Netherlands

This article considers the Court of Justice of the European Union's assessment and regulation of risks of discrimination in the context of algorithmic profiling based on Passenger Name Records data (PNR data). On the June 21, 2022 the court delivered a landmark judgment in *Ligue des Droits Humains* pertaining to discrimination and algorithmic profiling in a border security context. The CJEU identifies and seeks to regulate several risks of discrimination in relation to the automated processing of PNR data, the manual review of the results of this processing, and the resulting decisions taken by competent authorities. It interpreted whether the PNR Directive that lays down the legal basis for such profiling was compatible with the fundamental right to privacy, the right to data protection, and the right to non-discrimination. In its judgment, the CJEU seems to insufficiently assess various risks of discrimination. In particular, it overlooks risks relating to data quality and representativeness, automation bias, and practical difficulties in identifying discrimination. The judges also seem to prescribe safeguards against discrimination without guidance as to how to ensure their uniform and effective implementation. Such shortcomings can be observed in relation to ensuring the non-discriminatory nature of law enforcement databases, preventing indirectly discriminatory profiling practices based on collected PNR data, and configuring effective human-in-the-loop and transparency safeguards. This landmark judgement represents an important step in addressing algorithmic discrimination through CJEU adjudication. However, the CJEUs inability to sufficiently address the risks of discrimination in the context of algorithmic profiling based on the PNR Directive raises a broader concern. Namely, whether the CJEU is adequately equipped to combat algorithmic discrimination in the broader realm of European border security where algorithmic profiling is becoming increasingly commonplace.

KEYWORDS

algorithmic profiling, discrimination, PNR, artificial intelligence, law enforcement

1. Introduction

Law enforcement agencies (LEAs) are increasingly turning to algorithmic profiling technologies to process greater amounts of data. They hope that this will assist them in efficiently and effectively detecting and preventing crime (Dimitrova, 2022, p. 304). Algorithmic profiling for law enforcement proposes can be described as the process of generating and using profiles composed of indicators to process large quantities of data and thereby guide surveillance decisions (European Union Agency for Fundamental Rights, 2018b, p. 17, 19). The use of such technologies enables law enforcement agencies to, both reactively and proactively, target individuals or groups that are deemed to pose the highest risk of committing or having committed a crime (European Union Agency for Fundamental Rights, 2018b, p. 18, 19).

Within the European Union, the 2016 Passenger Name Records Directive (hereafter PNR Directive) provides a legal basis for the algorithmic profiling of passengers based on passenger name records data (hereafter PNR data) for the purpose of preventing, detecting, investigating, and prosecuting serious crime and terrorist offenses (Migration and Home Affairs, 2022). PNR data refers to data provided to air carriers by passengers. This can include information such as travel dates and itineraries, ticket information, contact information, payment information, and seat and baggage information (Migration and Home Affairs, 2022). On the basis of the PNR directive, this data is transferred prior to a flight's departure to Passenger information units (hereafter PIU) within each Member State (Directive 2016/681, 2016 Art. 4, 6). The PIU's then automatically process the PNR data against relevant databases as well as pre-established risk indicators in order to identify potential threats and guide surveillance decisions at the border (European Commission, 2020b, p. 24; United Nations, 2021; Directive 2016/681, Art 4, 6; Dimitrova, 2022, p. 310).

While such profiling practices and technologies promise to be useful, their irresponsible use has been found to present risks of discrimination which can clash with the right to non-discrimination (Borgesius, 2020, p. 1574–1576). Such discriminatory systems result in the undermining of trust by those under surveillance, as well as hindering the effectiveness and accuracy of surveillance activities (European Union Agency for Fundamental Rights, 2018b, p. 38, 39). In the context of algorithmic profiling based on PNR data, concerns of discrimination have also been raised in public and academic discourse. These concerns relate in particular to the advanced assessment procedure used to process PNR data against various databases and risk criteria, the manual review of the output of the profiling, and the decisions taken by authorities based on this procedure (Geulen and Klinger, 2019, p. 29; Privacy First, 2019; EpicenterWorks, 2020; Olsen, 2020; Gerards and Brouwer, 2022). In *Ligue des Droits Humains*, the CJEU assesses these risks and prescribes several safeguards to mitigate them (Opinion of A.G. Pitruzzella in Ligue des Droits Humains, 2022).

In light of this landmark judgment, the following research question will be explored: How does the CJEU assess and regulate risks of discrimination in the context of algorithmic profiling based on PNR data, and can its capacity for regulating algorithmic profiling technologies through adjudication be improved? In order to answer this question, the CJEU's assessment of risks of discrimination and prescribed regulatory safeguards will be delineated and analyzed. In particular, it will be considered if the risks of discrimination were adequately assessed and if the prescribed safeguards are fit for the purpose of mitigating the risks of discrimination present in the PNR context. These insight are then used to reflect more generally on the ability of the CJEU to effectively combat algorithmic discrimination through adjudication in the context of algorithmic profiling in a European border security context (Opinion of A.G. Pitruzzella in Ligue des Droits Humains, 2022).

This article responds to a lack of robust academic literature surrounding PNR following *Ligue des Droits Humains* that examines the issue of algorithmic discrimination (Olsen, 2020; Glouftsios and Leese, 2023). In answering the central research question, the CJEU's assessment of risks of discrimination and prescribed regulatory safeguards will be delineated on the basis of the *Ligue des Droits Humains* case and Advocate General Pitruzella's opinion on the case (Opinion of A.G. Pitruzzella in Ligue des Droits Humains, 2022). In delineating the concepts relevant to this paper and in conducting the analysis, academic and gray literature, such as blog articles, will be used. In addition, relevant legislation, governmental and non-governmental reports, and recent case law and preliminary references pertaining to the PNR context will be used to also carry out a normative analysis.

In section 2, the regulatory framework of algorithmic profiling and discrimination in the context of PNR will be described. In this section, algorithmic profiling and the legal basis for the use of such technologies as laid down by the PNR Directive will be delineated. Subsequently, the legal framework regulating algorithmic discrimination, both as prescribed by human rights standards and the PNR directive will be explored. Lastly, the role of courts in regulating algorithmic discrimination will be discussed and *Ligue des Droits Humains* will be introduced. In section 3, the CJEU's assessment and regulation of risks of discrimination in the context of algorithmic profiling will be analyzed. This will be done by delineating and subsequently analyzing the CJEU's assessment and regulation of risks within each of the three stages of the profiling process. Namely, the advanced assessment of passengers through the analysis of PNR data against relevant databases and predetermined criteria, the manual review of the results of the advanced assessment, and the decisions taken based on the advanced assessment and manual review. In section 4, the analytical insights from section 3 will be used to reflect on the broader challenges that exist in regulating risks of algorithmic discrimination through adjudication and suggestions to address these challenges will be delineated.

2. The regulatory framework governing algorithmic profiling and discrimination in the context of passenger name records

2.1. Algorithmic profiling and the PNR directive

LEAs tasked with controlling the borders must make a distinction between conventional travelers and potential criminals (Dekkers et al., 2019, p. 238). Profiling plays a crucial role

in making such distinctions. Profiles composed of criteria or indicators relevant to assessing the risk of someone engaging in or having engaged in criminalized behavior are used to inform surveillance decisions (European Union Agency for Fundamental Rights, 2018b, p. 15). Such criteria can be based on predictive characteristics relevant for proactively identifying persons not yet known to law enforcement that may be engaging or intend to engage in criminalized behavior (European Union Agency for Fundamental Rights, 2018b, p. 18). Today, predictive characteristics are often based on patterns and correlations found in datasets through data mining techniques and are increasingly being used to inform surveillance profiles and decisions at the border (Custers, 2013, p. 11–13; European Union Agency for Fundamental Rights, 2018b, p. 19; Eder, 2020, p. 27; Dimitrova, 2022, p. 306). Furthermore, criteria can also be based on intelligence relevant to identifying specific individuals already suspected by law enforcement of having committed a crime. For example, the presence of a person in a national, international, or European database pertaining to persons sought by law enforcement would indicate that the person in question likely engaged in criminalized behavior, thereby warranting their apprehension or additional surveillance (European Union Agency for Fundamental Rights, 2018b, p. 18).

Algorithmic profiling refers to the process of using algorithmic systems to automatically process data against such risk criteria in order to guide surveillance decisions (Custers, 2013, p. 11–13; European Union Agency for Fundamental Rights, 2018b, p. 19; Eder, 2020, p. 27). Other terms often used in literature and practice when referring to similar processes are for example, risk assessments/profiling, automated processing, automated/algorithmic decision-making, behavioral analysis, and intelligence-led or data-driven policing (Custers, 2013, p. 11; Darroch and Mazerolle, 2013, p. 22–23; Dekkers and van der Woude, 2017; European Union Agency for Fundamental Rights, 2018b, p. 19–20; Dekkers et al., 2019; European Commission, 2020b; Pesch et al., 2022). Despite these various terms referring to similar processes, the differences in terminology can result in differing pictures, expectations, and thoughts about the process or system in question (Langer et al., 2022 p. 2–3). To avoid such confusion in this paper, algorithmic profiling is used in this paper to refer to the automated processing of PNR data against both relevant databases and predictive criteria in order to assess the risk of terrorism and serious crime posed by passengers and thereby guide surveillance decisions.

The PNR directive provides the legal basis for the collection, retention, processing, and use of passenger name records for the purpose of preventing, detecting, investigating, and prosecuting terrorist offenses and serious crimes (Migration and Home Affairs, 2022). Terrorism refers to various acts that are committed with the aim of intentionally causing intimidation of a population, forcing a government or international organization to act or refrain from acting in a certain way, or destabilize or destroy the fundamental structures of a country or international organization (Directive 2016/681, 2016 recital para 12; Directive 2017/541, 2017, Art. 3). Serious crime refers to crimes such as the trafficking of humans, drugs, and weapons, money laundering, cybercrime, corruption, murder, and kidnapping that are punishable by at least 3 years imprisonment in a Member State (Directive 2016/681, 2016, Annex II).

Data for this purpose that can be collected by air carriers under the PNR Directive includes travel itinerary, address and contact information, travel agencies used, the travel status of passengers, baggage information, general remarks including information related to unaccompanied minors, and any changes to these categories of data (Directive 2016/681, 2016, Annex I). According to the PNR Directive, Member States must ensure that air carriers collect and transfer PNR data related to passengers on extra-EU flights, and in justified instances, intra-EU flights, to their national Passenger Information Unit (PIU), 24–48 h prior to the departure of the flight [Directive 2016/681, 2016, Art. 4, 8(3), recital para 10]. Once the data is received, PIUs automatically assess, process, and analyze these data against risk profiles composed of predetermined criteria, as well as relevant databases in order to guide surveillance toward those posing the highest risk of terrorism or serious crime (Directive 2016/681, 2016, Art. 6). In practice, as delineated in *Ligue des Droits Humains*, this process occurs via an advanced assessment procedure.

The first stage of the advanced assessment procedure involves automatically assessing the received PNR data against relevant databases and a set of predetermined criteria to identify persons involved in terrorist offenses or serious crime (Opinion of A.G. Pitruzzella in Ligue des Droits Humains, 2022, para. 176, 177). The databases can be on the national, European, or international level and pertain to "persons or objects sought or under alert," or otherwise relevant to combating serious crime and terrorism [Directive 2016/681, 2016, Art 6(3)(a)]. On the national level this encompasses law enforcement databases pertaining to suspected or known criminals. On the European level this includes, for example, the SIS II database which is used to check alerts relating to persons or objects, and on the international level the Interpol databases are of relevance to identifying criminals and crimes (Dimitrova, 2022, p. 310; Interpol, 2023; Migration and Home Affairs, 2023). The predetermined criteria used to automatically assess the risk of passengers can be based on, for example, travels booked with travel agencies or credit cards used by traffickers, inconvenient and suspicious travel patterns and prices, and discrepancies between baggage and passenger itinerary (European Commission, 2020b, p. 24). The second stage involves manually reviewing any positive matches to verify and decide whether actions must be taken by competent authorities in response to the match (Case C-817/19, 2022, para. 176–177). The list of competent authorities who may receive or request the results of the automated processing pertains to those adopted by a Member State, other PIU's, and Europol (Directive 2016/681, 2016, Art. 7, 9, 10).

In terms of the technical systems used for the automatic assessment of PNR data, there is a lack of publicly available information specifying how exactly these systems work. For example, in the Netherlands, the Travel Information Portal is used as a gateway for the collection of passenger name records, their storage and depersonalization, and their processing and analysis (Staatscourant, 2019, article 3 and 5; Ministry of Justice and Security, 2019). However, there is a lack of further technical specification regarding the role of the portal in generating assessment criteria, and the technical aspects of the assessment of PNR data against both

the predetermined criteria and relevant databases (Irion and Romy, 2021, p. 42, 43). This lack of technical specification is a limitation for this research as it hinders the ability to provide in depth analysis of concrete algorithmic systems used within Member State PIU's. In light of this limitation, this paper focuses on introducing arguments surrounding risks of algorithmic discrimination in the PNR context based on publicly available information regarding the algorithmic profiling process within PIU's.

2.2. The legal framework regulating algorithmic discrimination

Algorithmic profiling technologies are not immune to risks of discrimination (Borgesius, 2020, p. 1574–1576). Discrimination in this paper refers to unfair and unethical forms of differentiation that clash with or violate the right to non-discrimination (European Union Agency for Fundamental Rights, 2018b, p. 19–380; Borgesius, 2020, p. 1573). The right to non-discrimination under EU law is enshrined in article 21 of the Charter of Fundamental Rights of the European Union (CFEU) (Charter of Fundamental Rights of the European Union, 2000, Art. 21). This article corresponds to article 14 of the European Convention on Human Rights (ECHR) [European Convention on Human Rights, 1953, Art. 14; Charter of Fundamental Rights of the European Union, 2000, Art. 52(3); (Stirn and Bjorge, 2017), p. 75, 76; European Union Agency for Fundamental Rights, 2023].

The right to non-discrimination firstly prohibits direct discrimination which refers to the less favorable treatment of a person based on a protected characteristic such as sex, national origin, race, religion, or ethnicity (European Union Agency for Fundamental Rights, 2018a, p. 43, 155, 161). In the context of algorithmic profiling, such direct discrimination can be constituted and violate the right to discrimination where race and ethnicity are used as selection criteria to guide surveillance decisions at the border (Abdul-Aliyeva and van Eijk, 2023; Gerechtshof Den Haag, 2023). Under the right to non-discrimination, the use of seemingly neutral practices or rules that has the effect of placing people or groups at a disadvantage constitutes indirect discrimination and is also prohibited (European Union Agency for Fundamental Rights, 2018a, p. 53, 155, 161). Algorithmic profiling could lead to indirect discrimination if criteria that seem neutral, such as flying to or from a specific country, were unjustifiably incorporated into a risk profile and led to the disproportionate selection of persons with a specific background (Geulen and Klinger, 2019, p. 29; Netherlands Institute for Human Rights, 2021, p. 11, 18–19). According to the right to non-discrimination, differences in treatment based on protected characteristics are unjust and must be rebutted with proof that the difference in treatment is not based on these characteristics, or is justifiable (Gerards and Borgesius, 2022, p. 56).

The right to non-discrimination itself contains the substantive prohibition of discrimination. However, the right to equal treatment, the right to an effective remedy, and the right to data protection and privacy together contribute to important pillars safeguarding this prohibition (European Union Agency for Fundamental Rights, 2018b, p. 19–38; Borgesius, 2020, p. 1576–1581; Eder, 2020; European Union Agency for Fundamental Rights, 2020, p. 57–69, 75, 76; European Commission, 2020a, p. 9, 10). The right to equal treatment acts as a catch-all category to ensure that any differences in treatment stemming from a risk profile must be reasonable, fair, and can be reviewed by a court (Eder, 2020, p. 32–35, 40–44; Gerards and Borgesius, 2022, p. 56, 57). The right to an effective remedy sets important standards for effective access to justice in light of potentially discriminatory decisions based on algorithmic profiling systems in a border security context (European Union Agency for Fundamental Rights, 2020, p. 57, 58, 75–78; Amnesty International, 2023, p. 36, 37).

Furthermore, data protection legislation and the right to privacy place important safeguards on the collection and processing of personal data in the context of algorithmic profiling that contribute to safeguarding the prohibition of discrimination (Borgesius, 2020, p. 1578–1580). For example, the Law Enforcement Directive regulates the processing of protected categories of data, the use of automated processing technologies such as profiling, and the governance of risks associated with the use of automated processing technologies (Directive 2016/680, 2016, Art. 10, 11, 27). Furthermore, the retention, generation, and use of information in a surveillance context to differentiate between people and infer specific aspects of one's personal life, such as their ethnic origin, can also violate the right to privacy (Eder, 2020, p. 30–32; European Court of Human Rights, 2022, p. 8, 48, 56, 60–62, 72, 73). Thus, while a case may be brought under the right to privacy and data protection, the issue of discrimination may still be dealt with within the case as an issue related to privacy and data protection rather than non-discrimination (Gellert et al., 2013; Autoriteit Persoonsgegevens, 2020; The Hague District Court, 2020; Case C-817/19, 2022).

The PNR Directive itself also contains a number of safeguards against discrimination in the context of the automated processing and use of PNR data. Firstly, in the preamble, it is emphasized that the directive should be implemented in accordance with the right to non-discrimination (Directive 2016/681, 2016, recital para 20). It makes explicit that no decision based on the automated processing of PNR data should discriminate on grounds such as "sex, race, color, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation" (Directive 2016/681, 2016, recital para 36). Article 6(4) further specifies that assessments prior to the arrival of passengers against the predetermined criteria must be carried out non-discriminatorily and cannot be based on the list of protected grounds [Directive 2016/681, 2016, Art. 6(4)]. These criteria must be defined in a way that minimizes the incorrect identification of passengers as presenting a risk and must be reviewed regularly (Directive 2016/681, 2016, recital para 7, Art. 6(5); European Commission, 2020b, p. 6–7). Furthermore, article 13(4) stipulates that processing PNR data in a manner that reveals sensitive information corresponding to the list of protected grounds is prohibited and must be deleted immediately [Directive 2016/681, 2016, Art. 13(4)].

Any positive matches based on the automated processing must subsequently be manually reviewed prior to a decision being taken since the processing [Directive 2016/681, 2016, recital

para 7, Art. 6(5), 7(6)]. Article 7(6) stipulates that the non-discrimination principle also applies to any subsequent decisions taken by competent authorities relying on the results of the automated processing of PNR data [Directive 2016/681, 2016, Art. 7(6)]. Finally, article 13(1) provides a judicial remedy mechanism by stating that all passengers have the right to the protection, access, rectification and erasure of their personal data, and the right to judicial redress and compensation [Directive 2016/681, 2016, Art. 13(1)].

2.3. Regulating algorithmic discrimination through adjudication

As the right to non-discrimination is regulated by EU law and several articles in the PNR directive, the legislative framework enables passengers to invoke their rights against a public body. This enables the assessment of the legality of possible discriminatory algorithmic profiling. Courts in these instances issue binding interpretations of broad legal standards, such as the right to non-discrimination and clarify their applications to specific situations, such as algorithmic profiling at the border (Chalmers et al., 2019, p. 180; Wachter et al., 2020, p. 19, 20; Fairfield, 2021, p. 55–59). In this sense, courts provide much-needed guidance and legal certainty to organizations relying on algorithmic profiling technologies regarding when the use of such technologies may be deemed just or unjust (Fairfield, 2021, p. 17–20; Gerards and Borgesius, 2022, p. 7). This can be done by, for example, clarifying what constitutes justified forms of unequal treatment or discrimination, prohibiting certain profiling practices, and prescribing necessary safeguard mechanisms in order to comply with fundamental rights (Amnesty International, 2021; Gerards and Borgesius, 2022, p. 34; Case C-817/19, 2022; Gerechtshof Den Haag, 2023). Courts thus safeguard the right to non-discrimination by developing legislative standards in response to specific cases (Gerards and Borgesius, 2022, p. 18). As such, court decisions must subsequently be considered when designing, implementing, and deploying algorithmic profiling systems in the future (Gerards and Borgesius, 2022, p. 34).

Regarding the right to non-discrimination, the CJEU has thus far produced no cases in which discrimination in the context of algorithmic profiling based on PNR data has been addressed. As such, *Ligue des Droits Humains* is a landmark judgement in which the Court of Justice of the European Union (hereafter CJEU) adjudicates on this matter (Case C-817/19, 2022). Prior to *Ligue des Droits Humains*, the aforementioned issue had been only briefly touched upon in Opinion 1/15 CJEU. In Opinion 1/15 CJEU, due to incompatibility with articles 7 and 8 CFEU, the CJEU prevented the conclusion of an agreement between the EU and Canada that would enable the transfer and processing of PNR data (Opinion 1/15 CJEU, 2016). Regarding discrimination, the CJEU stated that such an agreement must ensure that the advanced assessment procedure is carried out in a manner that targets, in a non-discriminatory manner, those reasonably suspected of terrorism or serious criminality (Opinion 1/15 CJEU, 2016).

In *Ligue des Droits Humains*, the CJEU responds to a preliminary reference submitted by Belgium. The Court considered the validity of the directive in light of the right to privacy and data protection, namely article 7, 8 and 52(1) of the Charter of Fundamental Rights. However, the Court also interprets various aspects of the PNR Directive in light of the right to non-discrimination as enshrined in article 21 of the Charter. In particular, the CJEU goes further than *Opinion 1/15 CJEU* as it assesses in greater depth the risks of direct and indirect discrimination associated with algorithmic profiling based on PNR data and prescribes a number of safeguards intended to mitigate these risk. The judgment and prescribed safeguards carry consequences for the PNR context, but may also be of relevance to other systems under development or being used for profiling at EU borders (Gerards and Brouwer, 2022). Such systems include the under development Entry Exit System and the European Travel Information System, as well as a number of databases such as SIS II, VIS, and Eurodac (Dimitrova, 2022, p. 306).

3. Analyzing the CJEU's assessment and regulation of risks of discrimination in algorithmic profiling based on PNR data

In *Ligue des Droits Humains*, the court addressed the matter of non-discrimination in relation to the algorithmic profiling of passengers by PIU's. The profiling process consists of three stages. Namely, the automated processing of PNR data against relevant databases and predetermined criteria, the manual review of the results of processing, and decisions taken based on this process. At each stage of the process, the CJEU's identification of risks and prescribed safeguards will be delineated and subsequently analyzed. This is done to assess whether the CJEU sufficiently identifies the risks of discrimination, and if the prescribed safeguards are fit for the purpose of governing of these risks. This analysis draws on literature, reports from the European and National level, and information from civil society groups.

3.1. Processing PNR data against relevant databases and predetermined criteria

3.1.1. PNR data

The CJEU acknowledged in its judgment that when taken together, the categories of PNR data that can be collected and automatically processed under the PNR Directive, are liable to reveal sensitive information about passengers (Case C-817/19, 2022, para 100). Such sensitive data refers to PNR data that may reveal a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation (Case C-817/19, 2022, para 120). Additionally, a passengers name, address, or travel dates corresponding to specific holidays could act as proxies enabling assumptions to be made about ethnicity, religious affiliation or nationality and used to evaluate the risk posed by passengers (Opinion of A.G. Pitruzzella in Ligue des Droits Humains, 2022, para 184). Of particular relevance to discrimination, it was found that the category of 'general remarks' left room for the inclusion of information, such as

dietary preferences or requests for assistance, that could indirectly reveal sensitive information (Opinion of A.G. Pitruzzella in Ligue des Droits Humains, 2022, para 134, 135, 179, 180).

The CJEU went on to say that the data collected on the basis of PNR Directive must be limited to what is strictly necessary for combating serious crime and terrorism and exclude sensitive data (Case C-817/19, 2022, paras 117, 128, 130). Furthermore, Advocate General Pitruzella stated that the obligation to exclude information revealing sensitive data applies already from the collection of data and that the obligation on PIU's to delete such information is merely a safeguard against if air carriers send it by mistake (Opinion of A.G. Pitruzzella in Ligue des Droits Humains, 2022, paras 179, 181). The CJEU went on to interpret a number of categories of data listed in Annex I to meet the requirements of being sufficiently clear and precise in order to be restricted to what is strictly necessary in light of the right to privacy and data protection (Case C-817/19, 2022, para 129, 130). In particular the problematic category of 'general remarks' was interpreted to restrict the scope of information that could be collected and transferred to PIU's (Case C-817/19, 2022, para 135). The CJEU thus decided that through interpretation of this category that only the information explicitly listed under the heading could be collected (Case C-817/19, 2022, para 136).

3.1.1.1. Analysis of the CJEU's risk assessment and prescribed safeguards

In relation to the PNR data that may be collected on the basis of the PNR Directive under Annex I, three key risks in relation to the data categories that could be collected and automatically processed were identified by the CJEU. Namely, that PNR data when taken together can reveal sensitive information, the risk of indirect discrimination through proxies, and the risk of sensitive information being included in free text headings (Case C-817/19, 2022, para 100, 120, 134, 35; Opinion of A.G. Pitruzzella in Ligue des Droits Humains, 2022, para 179, 180, 184). These same risks have been identified and delineated in public and academic discourse (Olsen, 2020, p. 19–20; Geulen and Klinger, 2019, p. 29; Court of Justice of the European Union, 2019, p. 20–22; Court of Justice of the European Union, 2020b, p. 5; Court of Justice of the European Union, 2020a; Gerards and Brouwer, 2022).

With regards to the prescribed safeguards addressing these issues, firstly a challenge arises in relation to the exclusion of sensitive data. In practice some categories of information such as name, address, or travel dates, that could act as a proxy and enable sensitive inferences simply cannot be excluded without rendering the data useless for assessment (Olsen, 2020, p. 19, 20). Additionally, without the use of statistical analyses it may not always be clear which information acts as a proxy or is liable to indirectly lead to discrimination (Olsen, 2020, p. 20). Furthermore, Advocate General Pitruzella stipulates that this obligation applies to airline carriers collecting the PNR data (Opinion of A.G. Pitruzzella in Ligue des Droits Humains, 2022, para 179, 181). In practice this is challenging as airline carriers are primarily concerned with efficient and cost effective passenger transport as opposed to collecting factually accurate data and guaranteeing its non-discriminatory nature (Glouftsios and Leese, 2023, p. 134). Finally, in relation to the category of "general remarks," the CJEU does take an important step in regulating the possibility to transfer sensitive data via such a free text heading (Case C-817/19, 2022, para 135, 136).

3.1.2. Relevant databases

The PNR directive enables comparing PNR data against relevant databases including persons or objects sought or under alert (Case C-817/19, 2022, para 183). The CJEU pointed out that the PNR Directive does not clarify which other databases can be deemed relevant, the nature of the data in those databases, their required relationship to the objectives pursued by the directive, and whether they may be public or private (Case C-817/19, 2022, para 183; Opinion of A.G. Pitruzzella in Ligue des Droits Humains, 2022, para 217). The term 'relevant databases' was thus found to be insufficiently clear and precise and leave room for the analyzing and mining of PNR data in combination with these databases (Case C-817/19, 2022, para 104, 183, 184; Opinion of A.G. Pitruzzella in Ligue des Droits Humains, 2022, para 217, 218). Such analysis and mining would enable further specific profiles and inferences to be made about the private life of all passengers and give rise to a feeling of seemingly constant surveillance (Case C-817/19, 2022, para 104, 183, 184; Opinion of A.G. Pitruzzella in Ligue des Droits Humains, 2022, para 217, 218).

However, the Court clarified that PNR data can only be compared to databases explicitly listed in the text of the directive, namely 'databases on persons or objects sought or under alert, in accordance with EU, international and national rules applicable to such databases' (Case C-817/19, 2022, para 187, 188). Additionally, the databases must be used for combating serious crime and terrorism and have at least an indirect link to air travel (Case C-817/19, 2022, para 191). The Court went on to state that the advanced assessment of PNR data against such databases must be compliant with the right to non-discrimination, and the entry of persons in these databases must also be done based on objective and non-discriminatory factors (Case C-817/19, 2022, para 189, 190).

3.1.2.1. Analysis of the CJEU's risk assessment and prescribed safeguards

The CJEU seems to implicitly recognize the risk that historically discriminatory policing practices, such as ethnic profiling, can be reflected in databases and consequently influence the assessment of PNR data against such databases (Rosenfeld and Richardson, 2019; EDRI, 2022). This can be especially problematic if these databases are also mined in order to contribute to formulation of predictive criteria that may reflect discriminatory policing practices (Huggins, 2021, p. 1065; Gerards and Brouwer, 2022; Thönnes, 2022). Additionally, where databases are made interoperable, as is increasingly the case in the EU, the chance of having access to and relying on biased and discriminatory data within one or more of these databases increases (European Union Agency for Fundamental Rights., 2017, p. 44; Sooriyakumaran and Jegan, 2020, p. 3–5; Statewatch, 2022).

Besides narrowing the scope of databases relevant to the advanced assessment procedure, the CJEU states that both the assessment of PNR data against relevant databases and the entry into the databases must not be discriminatory (Case C-817/19, 2022, para 189, 190). The CJEU thus tries to reduce the scope of databases that can be used to draw highly specific and potentially

sensitive inferences and guarantee their non-discriminatory nature (Case C-817/19, 2022, para 187, 88, 191). However, the CJEU places the onus on PIU's to ensure that the process is not discriminatory, and that the entry of persons into other databases is non-discriminatory. The CJEU offers no further guidance on this point, and it is therefore unclear how and to what extent the quality and non-discriminatory nature of "relevant databases" can be verified and guaranteed by PIU's (Sooriyakumaran and Jegan, 2020, p. 3–5; EDRI, 2022; Glouftsios and Leese, 2023, p. 127–133).

3.1.3. Predetermined criteria

Article 6(3)(b) of the PNR directive legislates for PNR data to be processed against a set of predetermined criteria [Directive 2016/681, 2016, Art. 6(3)(b)]. Firstly, the Court importantly acknowledged that when profiling based on predetermined criteria, a risk exists of both direct and indirect discrimination based on grounds protected by article 21 of the Charter and article 9(1) of the GDPR (Case C-817/19, 2022, para 120, 197, 199). Additionally, the Court found that besides the risk of discriminatory profiles, there was a general risk of predetermined criteria leading to incorrectly identifying passengers as a threat (Case C-817/19, 2022, para 106). Secondly, the court stipulated that the use of autonomous machine learning technologies would likely hinder the manual review of any positive matches by making it potentially impossible to understand why a passenger was selected for additional supervision (Case C-817/19, 2022, para 194, 195). Furthermore, the opacity of such systems would likely deprive data subjects of their right to an effective remedy and ability to challenge the non-discriminatory nature of the results of the system (Case C-817/19, 2022, para 195).

The Court addressed the identified risks by prescribing a number of safeguards to guarantee non-discriminatory nature of the predetermined criteria. Firstly, It was reiterated that these criteria 'are in no circumstance to be based on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation' (Case C-817/19, 2022, para 196). The Court argued that the phrase 'in no circumstances' covered both direct and indirect discrimination, and thus the criteria must not only be neutral in their wording but also should not place persons of a protected group at a disadvantage (Case C-817/19, 2022, para 197). Furthermore, the Court stated in addition to being non-discriminatory, the predetermined criteria must be defined so as to be based on the factual conduct of passengers, and minimize the amount of innocent people falsely identified as presenting a risk (Case C-817/19, 2022, para 203). Thus, the criteria must be regularly reviewed to ensure that they are still justified in their use, and not unnecessary by way of resulting in a high number of false positives (Case C-817/19, 2022, para 201). Secondly, with regards to the use of machine learning techniques, the Court stipulated that the term "pre-determined," precluded the use of self-learning artificial intelligence systems. Specifically, the Court prohibited the use of self-learning artificial intelligence technologies capable of modifying the assessment process, assessment criteria, and the weighting of those criteria without human intervention or review (Case C-817/19, 2022, para 194).

3.1.3.1. Analysis of the CJEU's risk assessment and prescribed safeguards

With regards to the predetermined criteria used in the profiling of passengers, the CJEU recognizes the risk of direct and indirect discrimination, problems of opacity related to the use of artificial intelligence technologies, and the need for accurate risk profiles (Case C-817/19, 2022, para 106, 120, 195, 197, 199). The Court firstly prescribes that the criteria must not lead to direct and indirect discrimination, and should be based on the factual conduct of passengers (Case C-817/19, 2022, para 196, 197). The reference to factual conduct seems to be aimed at preventing direct discrimination through profiling based on physical characteristics such as ethnicity, gender, and age (European Union Agency for Fundamental Rights, 2018b, 18). The CJEU however provides no guidance on the prevention of indirect discrimination. It thus falls to PIU's to operationalize this requirement in a uniform manner and exercise necessary due diligence to identify indirect discrimination (Olsen, 2020, p. 19, 20).

Secondly, the CJEU addresses the opacity associated with artificial intelligence by prescribing the safeguard of human intervention when relying on such technologies to modify the assessment process, predetermined criteria and their weighting (Case C-817/19, 2022; Gerards and Brouwer, 2022, para 194). With regards to discrimination, this is an important risk to acknowledge as black box systems can make it difficult to detect discriminatory effects, audit the system, and explain the workings of the system (Borgesius, 2018, p. 34, 35; Fountain, 2022, p. 6). Prescribing a human-in-the-loop safeguard can be an important safeguard against systems operating autonomously, and thus facilitate the understanding, challenging and communication of system outputs (Rosenfeld and Richardson, 2019, p. 680–683). However, here again, the CJEU provides no guidance on how this safeguard is supposed to be operationalized, which leaves it up to PIU's to configure their own safeguards. Such discretionary room assumes that PIU's are able to fill this discretion and design effective and uniform human-in-the-loop safeguards.

Thirdly, while the CJEU acknowledges the high rate of false positives, it overlooks the critical issue of data quality and quantity in relation to generating reliable and representative predetermined criteria based on PNR data (Case C-817/19, 2022, para 106). The European Council in 2022, points out that the trustworthiness of risk indicators relies heavily on the quality of data used to inform these indicators (Council of the European Union, 2022, p. 57). This is particularly problematic in the case of PNR data.

PNR data is declaratory in nature as it is filled in by passengers and transferred by air carriers that are primarily concerned with facilitating efficient travel as opposed to delivering high quality data sets (Glouftsios and Leese, 2023, p. 134). Thus, often the data received by PIU's is riddled with mistakes in the data, left out variables, and fictitious information such as names and passport numbers filled in the case of last minute changes to flight information (European Commission, 2020b, p. 42; Glouftsios and Leese, 2023, p. 134). Furthermore, PNR data and the results of its processing that are exchanged and received via request by other PIU's tends to be transferred unsystematically and in a piecemeal fashion (Glouftsios and Leese, 2023, p. 139). This makes interpreting this data and guaranteeing the reliability and

non-discriminatory nature of the data a challenge for other PIU's (Glouftsios and Leese, 2023, p. 139). Lastly, few tangible results related to the various forms of crime and terrorism have been achieved based on the PNR regime that would lend themselves to analysis and mining (Hypolite, 2018; Bundespolizei, 2020, p. 37, 69; Irion and Romy, 2021, p. 4–5, 9; Glouftsios and Leese, 2023, p. 137).

This insufficiency of data quality and quantity makes it difficult to analyze or mine the available PNR data and few results of its processing for the purpose of generating effective and representative profiles (Glouftsios and Leese, 2023, 132, 137, 138). Where this lack of data quantity and quality influences risk criteria, the risk of unwarranted and discriminatory suspicion being reflected in the algorithmic outputs and surveillance practices increases substantially (Privacy First, 2019). The CJEU seems to overlook the issue of insufficient data quality and quantity and how this may impact the effectiveness and representativeness of predetermined criteria. Thus, in the absence of good quality data sets informing the predetermined criteria, it may be required that profiles are generated on the basis of potentially biased experience of enforcement agents (Glouftsios and Leese, 2023, 132, 137, 138; Gerards, 2023).

3.2. Manual review of the results of the automated processing

In *Ligue des Droits Humains*, the Court reiterated that the automated analyses of PNR data present a certain margin of error due to the analyses being conducted, based on unverified data submitted by airlines, and predetermined assessment criteria (Case C-817/19, 2022, para 106). However, in the case of the PNR regime, this margin of error is particularly high, with five out of six passengers being incorrectly identified by automated means upon manual review Case C-817/19, 2022, para 106). The Court, in assessing the interference of the automated processing with the right to privacy and data protection, stated that the 'fairly substantial' amount of false positives threatened the appropriateness of the PNR system (Case C-817/19, 2022, para 123–125). In light of the inaccuracy associated with processing PNR data, the Court stressed that the appropriateness of the system as a whole is 'essentially dependent' on the effective functioning of the manual review and verification of the positive results of the advanced assessment (Case C-817/19, 2022, para 124).

The court introduced a number of safeguards regarding the manual review of any positive matches through the automated processing of PNR data. The court stipulated that the manual review of positive matches stemming from automated processing against relevant databases or pre-determined criteria, served to identify and remove false positives generally and exclude any discriminatory results (Case C-817/19, 2022, para 203). The manual review carried out by enforcement agents must therefore be guided by clear and precise rules laid down by Member State PIU's capable of ensuring compliance with the right to privacy, data protection and non-discrimination, (Case C-817/19, 2022, para 205, 206). These rules must ensure a 'uniform administrative practice' that safeguards passengers against any form of discrimination (Case C-817/19, 2022, para 205). The Court further explains that agents within a PIU must, on the basis of a set of clear and precise objective review criteria, firstly be able to effectively verify positive matches as a means to counter the "fairly substantial number of false positives" (Case C-817/19, 2022, para 206). Secondly, the objective review criteria must enable agents to verify the non-discriminatory character of the automated processing of PNR data, the predetermined criteria used, and the databases used (Case C-817/19, 2022, para 206). PIU's must also ensure that the manual review is documented, as well as all other processing activities of PNR data (Case C-817/19, 2022, para 207).

3.2.1. Analysis of the CJEU's risk assessment and prescribed safeguards

The CJEU acknowledges in its judgment that, five out of six passengers between 2018 and 2019 were incorrectly identified via automated processing as posing a threat once these signals were manually reviewed by PIU's (Case C-817/19, 2022, para 106). The European Commission stated that the requirement to review the matches generated by the algorithmic profiling system ensures the elimination of any such false positive matches and ensures that the PNR system delivers targeted results (European Commission, 2020b, p. 30). The CJEU, also takes this stance as it argues that the appropriateness of the system depends on the manual review effectively removing false positives and discriminatory results (Case C-817/19, 2022, para 124, 203). However, in prescribing a human review as a safeguard against inaccuracies, the CJEU seems to still ignore the underlying data issues and also overlook the issue of automation bias (Gerards, 2023).

Research has demonstrated that humans often overly rely on the output of algorithmic systems due to cognitive laziness, insufficient skills to challenge the output, and perceptions of superiority or infallibility of algorithms (Huggins, 2021, p. 1067; Alon-Barkat and Busuioc, 2023, p. 155). Additionally it has been demonstrated in literature that detrimental outcomes may also emerge in situations where enforcement agents selectively deviate or follow the output of algorithmic systems according to their own biases and discriminatory views (Green, 2022, p. 7, 8; Alon-Barkat and Busuioc, 2023, p. 155, 156; Thönnes, 2023). Thus, where the output of those automated systems are inaccurate, discriminatory, or otherwise biased, a risk exists that those verifying the matches overly rely or selectively adhere to the output of the algorithmic systems used (McDermott, 2019; Alon-Barkat and Busuioc, 2023). Lastly, reduced adherence to effective rules and procedures can negatively impact the quality of decisions taken by civil servants working with ICT systems (Busch and Zinner Henriksen, 2018, p. 11).

Though not mentioned in the judgment, in 2019 it was discovered that the automated system used to process PNR records in Germany had a false positive rate of 99.7% (Endt, 2019). Similarly, in Austria it was found that only 0.1% of hits from the automated system were actually correct (EpicenterWorks, 2020). The inaccuracies of the automated processing systems demonstrates that the predetermined criteria are not effective and accurate, which could, at least in part, be due to the underlying data quantity and quality issue used to inform the predetermined criteria (Council of the European Union, 2022, p. 57). These inaccuracies

increase the risk that inaccurate, biased, or discriminatory outputs may be reflected in the surveillance decisions taken. This risk is compounded as reviewing such false positives, according to Member State PIU's and the European Commission, 'significantly increases' the workload passenger information units (European Commission, 2020b, p. 46) and thereby the chances of errors. Furthermore, the CJEU does not provide parameters on how the manual review or the criteria guiding it should be formulated (Case C-817/19, 2022, para 203–207). In the absence of effective and uniform procedures for reviewing automated signals, a risk exists that enforcement agents may be more susceptible to errors stemming from a lack of effective rules and procedures (Busch and Zinner Henriksen, 2018, p. 11; Green, 2022, p. 8). Thus, a risk of errors and automation bias emerges due to unreliable data and profiling systems, a lack of prescribed procedures for reviewing the output, and the increased workload faced by enforcement agents within PIUs that are tasked with reviewing these signals.

3.3. Decisions based on the automated processing of PNR data

Subsequently the Court briefly devoted attention to the subsequent decisions taken by competent authorities on the basis of the automated processing of PNR data and manual review. Firstly, the CJEU highlighted that decisions taken on the basis of the advanced assessment that produce adverse legal effects on a person must not be taken solely on the basis of automated processing (Case C-817/19, 2022, para 208). Secondly, the Court stated that such decisions must be lawful and cannot be discriminatory (Case C-817/19, 2022, para 209). Thirdly, the CJEU highlighted the importance of passengers being enabled to exercise their right to judicial redress, in the event of a discriminatory decision being taken (Case C-817/19, 2022, para 210).

The Court firstly prescribed that competent authorities taking decisions that produce adverse legal effects for passengers must take into account and give priority to the result of the manual review of the positive match (Case C-817/19, 2022, para 208). Secondly, competent authorities must additionally be able to guarantee that the automated processing and subsequent manual review are non-discriminatory in nature (Case C-817/19, 2022, para 209). Thirdly, in the context of judicial redress, competent authorities must guarantee that the passenger concerned can understand the predetermined assessment criteria, systems, and manual review criteria to the extent that they are able identify possible discrimination and exercise their right to an effective remedy (Case C-817/19, 2022, para 210). Where such a remedy is exercised, save for cases of national security, both the court reviewing the legality and the concerned passenger must be able to examine the grounds and evidence that led to a decision being taken (Case C-817/19, 2022, para 211). Finally, the CJEU stated that, the data protection officer within the PIU, and national supervisory authority are also tasked with the role of monitoring that the processing of PNR data is not discriminatory (Case C-817/19, 2022, para 212).

3.3.1. Analysis of the CJEU's risk assessment and prescribed safeguards

The court firstly acknowledges that decisions taken by competent authorities cannot be solely based on the automated processing of PNR data and the decisions should be lawful and non-discriminatory (Case C-817/19, 2022, para 208, 209). The Court thus prescribes that preference is given to the manual review of the positive match, and that competent authorities must guarantee the non-discriminatory nature of the advanced assessment procedure (Case C-817/19, 2022, para 208, 209). As discussed under the previous section regarding the manual review, giving preference to the manual review does not guarantee the exclusion of false positives and discriminatory results. Competent authorities must not only give priority to the manual review but also guarantee its non-discriminatory nature, yet the CJEU is silent on how this is to be achieved. This formulation is rather strange as the criteria guiding the manual review to ensure the accuracy and non-discriminatory nature of processing are laid down by Member State PIU's themselves (Case C-817/19, 2022, para 205–206). As such it seems that competent authorities can at most simply check that the manual review was conducted according to the procedures laid down by PIU's, which does not per se guarantee the non-discriminatory nature of the advanced assessment.

Furthermore, the CJEU stated that passengers must be able to identify possible discrimination and exercise their right to judicial redress (Case C-817/19, 2022, para 210). The issue of being able to identify discrimination in the context of algorithmic profiling is crucial to ensuring the legal protection of passengers against discrimination. Identifying that one may be the victim of automated discrimination is difficult as it often requires statistical evidence, knowledge of the use of an algorithmic profiling system and its workings, and an understanding of the effects of a system (Borgesius, 2018, p. 19, 34; Wachter et al., 2020, p. 2). Thus, in order to effectively contest decisions based on algorithmic profiling systems, passengers must at least be aware that a profiling system is being used and have sufficient information about the system and its use that enables them to make a complaint (European Union Agency for Fundamental Rights, 2020, p. 13). While this is a procedural goal, it also entails that systems must be designed to be explainable to those affected by decisions stemming from the output (European Union Agency for Fundamental Rights, 2020, p. 13).

The CJEU recognizes this risk and prescribes a number of important safeguards to help facilitate the exercising of judicial redress in the context of discriminatory decisions. Namely, it prescribes that passengers, competent authorities, and courts, must be able to understand the advanced assessment procedure and reasons leading to a decision being taken (Case C-817/19, 2022, para 211). This safeguard is particularly important in the context of passenger name records as passengers are often not aware to begin with that they are being subjected to algorithmic profiling based on their submitted data (Gerards and Brouwer, 2022). Thus, the CJEU prescribes important safeguards to facilitate the awareness and understanding of the profiling process. Furthermore, requiring that passengers, competent authorities, and courts can understand the profiling process could act as an incentive for PIU's to document their processing activities and ensure that they are

understandable and communicable. However, difficulties may still arise for PIU's in determining which information to communicate and how to communicate it in a manner that enables the exercising of judicial remedies while still ensuring the security of the system (Rosenfeld and Richardson, 2019, p. 8; Varosanec, 2022, p. 98). Despite information being communicated, it may nonetheless be difficult for passengers to process and understand the information to the extent that they can identify discrimination (Varosanec, 2022, p. 97–99). In identifying indirect discrimination and proxies this may be especially difficult as it often requires statistical analysis demonstrating that a particular group has been discriminated against (European Union Agency for Fundamental Rights, 2018a, p. 25; Wachter et al., 2020, p. 2; Gerards and Brouwer, 2022).

3.4. Reflecting on the CJEU's regulation of algorithmic discrimination in *Ligue des Droits Humains*

This landmark judgement represents an important step in addressing algorithmic discrimination through CJEU adjudication, and contains some noteworthy positive aspects. Firstly, the CJEU assesses risks and prescribes safeguards against algorithmic discrimination throughout the profiling process relating to the automated profiling process, the manual review of the results, and the decisions subsequently taken. Such an approach is in line with the idea that discrimination through algorithmic profiling is the result of social and technical risks, as they are present and interact throughout various stages of the algorithmic profiling process (Marabelli et al., 2021; Tilburg University, 2021).

Within this process, the court identifies risks relating to direct and indirectly discriminatory PNR data and selection criteria, issues of opacity when using machine learning systems, the problem of false positives, and the need for algorithmic discrimination to be understandable and identifiable to external parties (Case C-817/19, 2022, para. 100, 106, 120–125, 134–135, 194–199, 210–212) The CJEU also prescribes important safeguards against algorithmic discrimination. In particular, it restricts the scope of open-text fields and relevant databases, highlights that selection criteria must be based on factual conduct, and prescribes that systems are understandable by those using them and external parties (Case C-817/19, 2022, para. 135–136, 187–189, 191, 210–212). Secondly, despite *Ligue des Droits Humains* being brought under the right to privacy and data protection, the CJEU also considered the validity of the PNR Directive under the right to non-discrimination (Case C-817/19, 2022). This highlights that the potentially discriminatory impact of algorithmic profiling technologies often affects - and therefore must be addressed through – the lens of more than one fundamental right (Borgesius, 2020; Eder, 2020).

This approach to identifying and regulating risks of algorithmic discrimination is generally of value. Yet in the judgment itself, the CJEU falls short in a number of ways. One such way is that the CJEU acknowledges some risks of discrimination, but simultaneously overlooks several key risks relating to algorithmic discrimination. Firstly, in the context of profiling against or based on relevant databases, the CJEU seems to implicitly acknowledge the risk of discriminatory data in such databases. However, it does not actually examine this risk and how it may be exacerbated by interoperable databases and the use of machine learning systems (Case C-817/19, 2022, para 189–190). Secondly, with regards to the predetermined criteria, the CJEU clearly acknowledges the problem of inaccurate predetermined criteria but directs no attention to how insufficient data quantity and quality may affect this problem and exacerbate discrimination (Council of the European Union, 2022, p. 57; Case C-817/19, 2022, para 106). Thirdly, the CJEU also states that the appropriateness of the PNR system depends on the proper functioning of the manual review, but seems oblivious to the factors that are likely to cause errors and automation bias (Case C-817/19, 2022, para 124).

The second, and perhaps most critical way that the CJEU falls short is in regards to the safeguards it prescribes against algorithmic discrimination. Firstly, the CJEU requires that PIU's and airline carriers exclude sensitive information, yet seems oblivious to the challenges associated with identifying indirectly discriminatory data as well as the organizational realities of PIU's and airline carriers (Case C-817/19, 2022, para 117, 128, 130; Opinion of A.G. Pitruzzella in Ligue des Droits Humains, 2022, para 179, 181). Secondly, with regards to profiling based on or against relevant databases, the CJEU states that the process and entry into the relevant databases should be non-discriminatory, yet offers no parameters on how PIU's should verify this (Sooriyakumaran and Jegan, 2020, p. 3–5; Case C-817/19, 2022, para 189–190; Glouftsios and Leese, 2023, p. 127–133). Thirdly, the court stated that pre-determined criteria must not be indirectly discriminatory, yet does not specify how this is to be achieved or demonstrated (Case C-817/19, 2022, para 196, 197). Thirdly, in the context of human intervention where artificial intelligence systems are used, and in the manual review of the advanced assessment, the CJEU provides no instructions to PIU's regarding the uniform configuration of this human-in-the-loop safeguard (Case C-817/19, 2022, para 194, 205, 206). Lastly, it remains up to PIU's to determine how to communicate information regarding the algorithmic profiling process to passengers seeking to bring a claim of discrimination and other relevant external parties (Case C-817/19, 2022, para 210).

Courts, such as the CJEU, have an important role to play in clarifying and facilitating the uniform application of broadly formulated legal standards, such as the right to non-discrimination, to specific situations (Chalmers et al., 2019, p. 180; Wachter et al., 2020, p. 19–20; Fairfield, 2021, p. 55–59). In *Ligue des Droits Humains*, the CJEU fails to offer the guidance and clarification necessary for facilitating a uniform approach to mitigating risks of discrimination in the context of algorithmic profiling based on PNR data (Gerards, 2023). The CJEU often prescribes broadly formulated safeguards without additional guidance as to their uniform operationalization. This places are tremendous amount of discretion on PIU's to operationalize them in a manner that uniformly safeguards the right to non-discrimination (Musco Eklund, 2021; EDRI, 2022).

This is challenging as the complexity of algorithmic discrimination necessitates multidisciplinary expertise within an organization to effectively identify and mitigate risks of discrimination in an ex-ante fashion (Marabelli et al., 2021; Tilburg University, 2021, p. 11–13). Additionally, a risk exists that PIU's may simply try to circumvent the safeguards in pursuit of increasing surveillance (Statewatch, 2022).

Beyond the scope of the PNR context, the shortcomings of the CJEU in clarifying the application of the right to non-discrimination to the context of algorithmic profiling may also transpose to a broader 'emerging European security architecture' (Thönnes, 2023). This security architecture is composed of increasingly interoperable databases coupled with the use of algorithmic profiling systems by organizations other than PIU's (Statewatch, 2022; Thönnes et al., 2023). Such profiling systems include the European Travel Information and Authorization System (ETIAS) and profiling based on the proposed regulation to prevent and combat child sexual abuse [Regulation COM (2022) 209 Final, 2022; Statewatch, 2022; Thönnes et al., 2023]. With regards to both of the aforementioned systems, similar to the PNR context, risks of algorithmic discrimination have also been raised (Pesch et al., 2022, p. 63–65; European Parliamentary Research Service, 2023). This increase in algorithmic profiling systems coupled with similar risks of algorithmic discrimination, demonstrates that a framework clarifying the application of the right to non-discrimination in this context is needed.

4. Suggestions for future regulation of algorithmic discrimination through adjudication

This paper highlights several ways in which the CJEU fell short in assessing and prescribing effective and uniform safeguards against algorithmic discrimination. Literature and practice highlights that these shortcomings could, at least in part, stem from a lack of expertise regarding algorithmic discrimination and experience in adjudicating on the matter of algorithmic discrimination. In particular, it has been highlighted that judges often lack the sociotechnical expertise necessary for understanding algorithmic profiling technologies, the associated risks of discrimination, and how to regulate these risks effectively (European Commission, Directorate-General for Justice and Consumers, Gerads and Xenidis, 2021, p. 119; Passchier, 2020, p. 920, 921; UNESCO, 2023). The lack of expertise regarding the regulation of algorithmic discrimination is also not particularly surprising, given a general scarcity of dedicated legislation and case law regulating algorithmic discrimination (European Commission, Directorate-General for Justice and Consumers, Gerads and Xenidis, 2021, p. 28). On the EU level there are likewise few cases addressing the right to non-discrimination in the context of algorithmic profiling and law enforcement at the border. Thus, insufficient expertise of the technology and its risks, coupled with a lack of regulatory experience may explain the shortcomings of CJEU in assessing and addressing risks of algorithmic discrimination in the PNR context.

Given the shortcomings of the prescribed measures in the PNR context and the presence of algorithmic discrimination risks in the "emerging European security architecture," it is inevitable that the CJEU will need to adjudicate on algorithmic profiling and discrimination again. As such, overcoming the challenge of expertise is imperative. In this regard, several initiatives can be identified to strengthen the capacity of judges and the CJEU when adjudicating on such cases in the future. Firstly, several initiatives exist that are aimed at educating and training judges about algorithmic discrimination in order increase their capacity to adjudicate on such matters. For example, UNESCO's Global Judge Initiative course on AI and the rule of law is being used to help educate judges on addressing issues of bias and discrimination in the context of AI UNESCO (2023). In the EU, the Justice, fundamentaL rIghts and Artifical intelligence (JuLIA) project aims to develop trainings and a handbook for judges adjudicating on matters pertaining to (semi-)automated decision making and fundamental rights, such as algorithmic discrimination (European Commission, 2021).

Secondly, human rights reports based on instances of algorithmic discrimination and relevant dedicated case law may offer inspiration for the prescription of regulatory safeguards at the European level. For example, the Netherlands Institute for Human Rights developed a framework based on instances of algorithmic discrimination and relevant case law that enables the assessment of discrimination in the context of risk-profiling (Netherlands Institute for Human Rights, 2021). Additionally, the European network of legal experts in non-discrimination wrote a report considering solutions for preventing and remedying algorithmic discrimination (European Commission, Directorate-General for Justice and Consumers, Gerads and Xenidis, 2021, p. 140–150). Finally, the Future of Privacy Forum published a report outlining how national courts and Data Protection Authorities have used the GDPR to regulate matters of algorithmic discrimination (Future of Privacy Forum, 2022). The combination of these sources can enable judges at the European level to prescribe effective safeguards against algorithmic discrimination based on past cases, best practices, and the application of complimenting human rights, such as the right to non-discrimination and data protection (Borgesius, 2020, p. 5–11).

Finally, the capacity of the CJEU to adjudicate on matters pertaining to algorithmic discrimination and the application of the right to non-discrimination can be bolstered by the use of experts. Judges in the CJEU may entrust individuals, bodies, authorities, committees, or other organizations with the task of giving expert opinions in order to enable the delivery of a judgment (Official Journal of the European Union, 2012, Art. 70; Official Journal of the European Union, 2015, Art. 96; European Parliament of the Council, 2016, Art. 25). Thus, where judges within the CJEU lack the necessary expertise to adequately assess risks of algorithmic discrimination or prescribe safeguards capable of facilitating the mitigation of these risks, the use of experts can help to bridge this knowledge gap (Riddell, 2013, p. 849, 869). Given that algorithmic discrimination is the product of social and technical factors interacting throughout the profiling process, it may be necessary to appoint experts from various disciplines (Sarker et al.,

2019, p. 696, 697; Ferrer et al., 2021; Marabelli et al., 2021, p. 2). In particular, experts in the sociotechnical, technical, legal, and public administration domain can provide insights relevant to delivering effective judgments as to the application of the right to non-discrimination in an algorithmic profiling and discrimination context (Sarker et al., 2019, p. 696, 697; Marabelli et al., 2021, p. 2, 4).

5. Conclusion

In *Ligue des Droits Humains* the CJEU delivered a landmark judgment at the European level which tackles the issue of discrimination in the context of algorithmic profiling based on PNR data. While the judgment focuses on the context of algorithmic profiling based on PNR data, the contents may carry implications for other profiling systems used or under development in the European Union. The CJEU identifies several risks of algorithmic discrimination in the profiling process pertaining to discriminatory data and selection criteria, the opacity of AI systems, and issues of transparency. It also introduces measures regulating open-text fields and databases, selection criteria, and the need for systems to be understandable and discrimination to be identified. The judgment importantly highlights that regulating discrimination resulting from algorithmic profiling requires using more than one fundamental right – such as privacy, data protection, non-discrimination, and a right to an effective remedy – to implement safeguards throughout the profiling process.

However, the judgment also underscores the challenges of regulating algorithmic discrimination through adjudication. In *Ligue des Droits Humains*, the CJEU falls short in the assessment of the risks of discrimination. This is reflected in several instances where the CJEU overlooks important risks of algorithmic discrimination. These risks pertain to historically biased and discriminatory in law enforcement databases, issues of data quality and quantity, and automation bias and human errors. The CJEU subsequently fails to prescribe safeguards to regulate risks of discrimination that were overlooked. Additionally, where risks of discrimination were correctly identified, the CJEU prescribes safeguards that are rendered somewhat ineffective due to a lack of clarity as to their operationalization. Problematic safeguards can be observed in relation to ensuring the accuracy and non-discriminatory nature of PNR data and relevant law enforcement databases, preventing the use of indirectly discriminatory profiles, configuring effective human-in-the-loop and transparency safeguards. This results in a considerable amount of discretion in PIU's and a lack of guidance regarding the application of the right to non-discrimination when developing effective and uniform risk mitigation strategies. The shortcomings translate to the broader context of the various systems being used and developed within the European Union, thus leading to a broader issue of poor legal protection in the context of algorithmic discrimination.

Finally, the judgment reflects a challenge regarding the extent to which courts have the expertise and experience to prescribe safeguards that effectively regulate algorithmic discrimination. Here three suggestions are offered to address these issues of expertise and experience. Firstly, educating judges through trainings and courses centered around algorithmic discrimination and adjudicating on such matters. Secondly, using human rights reports based on instances of algorithmic discrimination and relevant dedicated case law to help CJEU judges in the formulation of effective safeguards against algorithmic discrimination. Finally, making use of experts from various disciplines to bridge knowledge gaps when assessing and addressing algorithmic discrimination. Addressing the issue of expertise and experience is crucial for the CJEU to effectively regulate algorithmic discrimination through adjudication in future and inevitable cases pertaining to algorithmic profiling.

Author contributions

The author confirms being the sole contributor of this work and has approved it for publication.

Conflict of interest

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

Abdul-Aliyeva, T., and van Eijk, G. (2023). Discriminerende risicoprofielen Waarom er een verbod moet komen op het gebruik van afkomst als selectiecriterium in (geautomatiseerde) risicoprofilering, Netherlands. *Juristenblad* 4.

Alon-Barkat, S., and Busuioc, M. (2023). Human–AI interactions in public sector decision making: "automation bias" and "selective adherence" to algorithmic advice. *J. Pub. Admin. Res. Theor.* 33, 1–14. doi: 10.1093/jopart/muac007

Amnesty International (2021). *Xenophobic Machines: Discrimination Through Unregulated Use of Algorithms in the Dutch Childcare Benefits Scandal*. London: Amnesty International.

Amnesty International (2023). *Veel Gestelde Vragen Over Rechtszaak Tegen de Koninklijke Marechaussee Vanwege Etnisch Profileren*. London: Amnesty International.

Autoriteit Persoonsgegevens (2020). *Belastingdienst/Toeslagen - De Verwerking van de Nationaliteit van Aanvragers van Kinderopvangtoeslag*. South Holland: Autoriteit Persoonsgegevens.

Borgesius, F. (2020). Strengthening legal protection against discrimination by algorithms and artificial intelligence. *The Int. J. Hum. Rights* 24, 10. doi: 10.31228/osf.io/673yv

Borgesius, F. Z. (2018). *Discrimination, Artificial Intelligence, and Algorithmic Decision Making*. London: Council of Europe.

Bundespolizei (2020). *Jahresbericht 2020*. Available online at: https://www.bundespolizei.de/Web/DE/Service/Mediathek/Jahresberichte/jahresbericht_2020_file.pdf?__blob=publicationFileandv=5 (accessed May 7, 2023).

Busch, P. A., and Zinner Henriksen, H. (2018). Digital discretion: a systematic literature review of ICT and street-level discretion. *Inf. Polity* 23, 50. doi: 10.3233/IP-170050

Case C-817/19 (2022). *Ligue des Droits Humains. EU:C:2022:491*.

Chalmers, D., Davies, G., and Monti, G. (2019). *European Union Law: Text and Materials, 4th Edn*. Cambridge: Cambridge University Press.

Charter of Fundamental Rights of the European Union (2000). *Charter of Fundamental Rights of the European Union*. 2012/C 326/02. European Union.

Council of the European Union (2022). *Final Report Future Group on Travel Intelligence and Border Management, Series Number 6767/22.3. March*. Brussels: Council of the European Union.

Court of Justice of the European Union (2019). *Summary of the Request for a Preliminary Ruling from Belgium in Case C-817/19*. Available online at: https://curia.europa.eu/juris/showPdf.jsf?text=anddocid=225831andpageIndex=0anddoclang=enandmode=reqanddir=andocc=firstandpart=1andcid=5910456 (accessed May 7, 2023).

Court of Justice of the European Union (2020a). *Request for a Preliminary Ruling From the Republic of Slovenia in Case C-486/20*. Available online at: https://curia.europa.eu/juris/document/document.jsf?text=anddocid=234637andpageIndex=0anddoclang=ENandmode=lstanddir=andocc=firstandpart=1andcid=1388203 (accessed May 7, 2023).

Court of Justice of the European Union (2020b). *Summary of the Request for a Preliminary Ruling from Germany in Case C-222/20*. Available online at: https://curia.europa.eu/juris/showPdf.jsf?text=anddocid=228843andpageIndex=0anddoclang=enandmode=reqanddir=andocc=firstandpart=1andcid=943328 (accessed May 7, 2023).

Custers, B. (2013). "Data Dilemmas in the Information Society: introduction and Overview," in *Discrimination and Privacy in the Information Society, Studies in Applied Philosophy, Epistemology and Rational Ethics*, *Vol. 3*, eds B. Custers, T. Calders, and B. Schermer (Berlin: Springer).

Darroch, S., and Mazerolle, L. (2013). Intelligence-led policing: a comparative analysis of organizational factors influencing innovation uptake. *Police Quarterly* 16, 3–37. doi: 10.1177/1098611112467411

Dekkers, T., and van der Woude, M. (2017). Acceptance denied: intelligence-led immigration checks in dutch border areas. *Eur. J. Polic. Stu.* 4, 2. doi: 10.5553/EJPS/2034760X2016004002005

Dekkers, T., and van der Woude, M., and Koulish, R. (2019). Objectivity and accountability in migration control using risk assessment. *Eur. J. Criminol.* 16, 273–254. doi: 10.1177/1477370818771831

Dimitrova, D. (2022). "Surveillance at the borders: Travellers and their data protection rights," *Research Handbook on Privacy and Data Protection Law Values, Norms and Global Politics*, eds E. González, R. van Brakel, and P. De Hert (New York, NY: Edward Elgar Publishing).

Directive 2016/680 (2016). *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (O.J. 2016., L119.)*

Directive 2016/681 (2016). *Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime (O.J. 2016, L 119).*

Directive 2017/541 (2017). *Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on Combating Terrorism and Replacing Council Framework Decision 2002/475/JHA and Amending Council Decision 2005/671/JHA (O.J. 2017, L 88).*

Eder, N. (2020). *Privacy, Non-Discrimination and Equal Treatment: Developing a Fundamental Rights Response to Behavioural Profiling. Algorithmic Governance and Governance of Algorithms: Legal and Ethical Challenges*, 23–48. Cham: Springer.

EDRI (2022). *Mass surveillance of External Travellers May Go on, Says EU's Highest Court*. Available online at: https://edri.org/our-work/mass-surveillance-of-external-travellers-may-go-on-says-eus-highest-court/ (accessed May 7, 2023).

Endt, C. (2019). *Falschtreffer bei Fluggastdaten: Jeder Siebte ist Unschuldig Verdächtig. Süddeutsche Zeitung*. Available online at: https://www.sueddeutsche.de/digital/fluggastdaten-bka-falschtreffer-1.4419760. (accessed May 7, 2023).

EpicenterWorks (2020). *Passenger Name Records*. Available online at: https://en.epicenter.works/thema/pnr-0 (accessed May 7, 2023).

European Commission (2020a). *White Paper on Artificial Intelligence - A European Approach to Excellence and Trust*. London: European Commission.

European Commission (2020b). *SWD(2020). 128 Final, Commission Staff Working Document Accompanying the Document [. . .] Report From the Commission to the European Parliament and The Council On the review of Directive 2016/681 on the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime*. London: European Commission.

European Commission, Directorate-General for Justice and Consumers, Gerads, J., and Xenidis, R. (2021). *Algorithmic Discrimination in Europe - Challenges and Opportunities for Gender Equality and Non-Discrimination Law*. Publications Office.

European Commission. (2021). *Justice, Fundamental Rights and Artificial Intelligence*. London: European Commission.

European Convention on Human Rights (1953). *Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as Amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5*.

European Court of Human Rights. (2022). *Guide on Article 8 of the European Convention on Human Rights*. Strasbourg: European Court of Human Right.

European Parliament and of the Council (2016). *Statute of the Court of Justice of the European Union, 31 August 2016*. Brussels: European Parliament and of the Council.

European Parliamentary Research Service (2023). *European Parliamentary Research Service Ex-Ante Impact Assessment Unit. Proposal for a Regulation Laying Down the Rules to Prevent and Combat Child Sexual Abuse Complementary Impact Assessment*. Brussels: EPRS.

European Union Agency for Fundamental Rights (2018a). *The European Court of Human, Rights and the Council of Europe. Handbook on European Non-Discrimination* Law. Vienna: FRA, ECtHR, CoE.

European Union Agency for Fundamental Rights (2018b). *Preventing Unlawful Profiling Today and in the Future: A Guide*. Vienna: European Union Agency for Fundamental Rights.

European Union Agency for Fundamental Rights (2020). *Getting the Future Right: Artificial Intelligence and Fundamental Rights*. Vienna: European Union Agency for Fundamental Rights

European Union Agency for Fundamental Rights (2023). *Article 21 - Non-Discrimination*. Available online at: https://fra.europa.eu/en/eu-charter/article/21-non-discrimination (accessed May 06, 2023).

European Union Agency for Fundamental Rights. (2017). *Fundamental Rights and Interoperability: EU Information Systems at Borders and for Security, Luxembourg: Publications Office of the European Union*. Available online at: https://fra.europa.eu/en/publication/2017/fundamental-rights-and-interoperability-eu-information-systems-borders-and (accessed May 7, 2023).

Fairfield, J. A. T. (2021). *Runaway Technology: Can Law Keep Up?* Cambridge: Cambridge University Press.

Ferrer, X., van Nuenen, T., Such, M., Coté, M., and Criado, M. (2021). Bias and discrimination in AI: a cross-disciplinary perspective. *IEEE Technol. Soc. Mag.* 40, 72–80. doi: 10.1109/MTS.2021.3056293

Fountain, J. (2022). The moon, the ghetto and artificial intelligence: Reducing systemic racism in computational algorithms. *Govern. Inf. Q.* 39, 101645. doi: 10.1016/j.giq.2021.101645

Future of Privacy Forum (2022). *Automated Decision Making Under the GDPR - A Comprehensive Case-Law Analysis*. Washington, DC: Future of Privacy Forum.

Gellert, R., de Vries, D., de Hert, K. P., and Gutwirth, S. (2013). *A Comparative Analysis of Anti-Discrimination and Data Protection Legislations*.Berlin: Springer.

Gerards, J. (2023). *Machine Learning and Profiling in the PNR System. VerfBlog*. Available online at: https://verfassungsblog.de/ml-pnr/ (accessed May 7, 2023).

Gerards, J., and Borgesius, F. (2022). *Protected Grounds and the System of Non-Discrimination Law in the Context of Algorithmic Decision-Making and Artificial Intelligence*. Denver, CO: Colorado Technology Law Journal.

Gerards, J. H., and Brouwer, E. R. (2022). *Ligue des droits Humains (HvJ EU, C-817/19) – Verduidelijking en vragen Naar Aanleiding van het Passenger-Name-Record (PNR)-systeem. European Human Rights Cases Update*. Available online at: https://www.ehrc-updates.nl/commentaar/212281?skip_boomportal_auth=1 (accessed May 6, 2023).

Gerechtshof Den Haag (2023). *ECLI:NL:GHDHA:2023:173*. Available online at: https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:GHDHA:2023:173 (accessed May 6, 2023).

Geulen, R., and Klinger, R. (2019). *Complaint and Application for a Temporary Injunction*. Available at: https://nopnr.eu/wp-content/uploads/2019/05/2019-05-13_PNR_lawsuit_GFF_Administrative_Court_De_Capitani.pdf (accessed May 13, 2019).

Glouftsios, G., and Leese, M. (2023). Epistemic fusion: passenger information units and the making of international security. *Rev. Int. Stu.* 49, 125–142. doi: 10.1017/S0260210522000365

Green, B. (2022). The flaws of policies requiring human oversight of government algorithms. *Computer Law Secur. Rev.* 45, 105681. doi: 10.1016/j.clsr.2022.105681

Huggins, A. (2021). Addressing disconnection: automated decision-making, administrative law and regulatory reform. *Univ. NSW Law J.* 44, 1048–1077. doi: 10.53637/WCGG2401

Hypolite, B. (2018). *API-PNR: An Overview of the French System and the Challenges Faced. WCO News.* Available online at: https://mag.wcoomd.org/magazine/wco-news-82/api-pnr-an-overview-of-the-french-system-and-the-challenges-faced/ (accessed May 7, 2023).

Interpol (2023). *Databases.* Available online at: https://www.interpol.int/How-we-work/Databases (accessed May 06, 2023).

Irion, K., and Romy, V. (2021). *PNR Act Review September 2021.* Amsterdam: University of Amsterdam.

Langer, M., Hunsicker, T., Feldkamp, T., König, C. J., and Grgić-Hlača, N. (2022). "Look! It's a computer program! It's an algorithm! It's AI!": does terminology affect human perceptions and evaluations of algorithmic decision-making systems?" in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*.

Marabelli, M., Newell, S., and Handunge, S. (2021). The lifecycle of algorithmic decision-making systems: Organizational choices and ethical challenges. *J. Strat. Inf. Syst.* 30, 101683. doi: 10.1016/j.jsis.2021.101683

McDermott, K. (2019). *An Explainer on the Base Rate Fallacy and PNR' Epicenter.Works.* Available online at: https://en.epicenter.works/content/an-explainer-on-the-base-rate-fallacy-and-pnr (accessed May 7, 2023).

Migration and Home Affairs (2022). *Passenger Name Record (PNR).* Available online at: https://home-affairs.ec.europa.eu/policies/law-enforcement-cooperation/passenger-data_en (accessed May 06, 2023).

Migration and Home Affairs (2023). *Schengen Information System (SIS).* Available online at: https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system_en

Ministry of Justice and Security (2019). *Reisgegevens Voor Opsporingsdiensten.* Available online at: https://www.justid.nl/onderwerpen/reisgegevens-voor-opsporingsdiensten (accessed May 06, 2023).

Musco Eklund, A. (2021). *Frontex and Algorithmic Discretion (Part I).* Berlin: Verfassungsblog.

Netherlands Institute for Human Rights (2021). *Discriminatie door risicoprofielen - Mensenrechtelijk Toetsingskader.* Amsterdam: Netherlands Institute for Human Rights.

Official Journal of the European Union (2012). *Rules of Procedure of the Court of Justice, 29 September 2012, L265./9.*

Official Journal of the European Union (2015). *Rules of Procedure of the General Court, 23 April 2015, OJ L 105.*

Olsen, H. P. C. (2020). *Beyond Data Protection Concerns – The European Passenger Name Record System. iCourts Working Paper Series, (207).*

Opinion 1/15 CJEU (2016). *Opinion 1/15 of the Court of Justice of the European Union of 26 July 2017 on the Draft PNR Agreement Between Canada and the European Union. 2017. EU:C:2017, 592.*

Opinion of A.G. Pitruzzella in Ligue des Droits Humains (2022). *Opinion of A.G. Pitruzzella in Ligue des Droits Humains EU:C: 2022, 65.*

Passchier, R. (2020). Digitalisering en de (dis)balans binnen de trias politica. *Ars Aequi* 69, 916–927.

Pesch, P., Dimitrova, D., and Boehm, F. (2022). "Data protection and machine-learning-supported decision-making at the EU border: ETIAS profiling under scrutiny," in *Privacy Technologies and Policy,* eds A. Gryszczyńska, P. Polański, and N. (Cham: Springer).

Privacy First. (2019). *PNR: Iedere Vliegtuigpassagier als Potentiële Verdachte?* Available online at: https://privacyfirst.nl/artikelen/pnr-iedere-vliegtuigpassagier-als-potentiele-verdachte/ (accessed May 7, 2023).

Regulation COM (2022) 209 Final (2022). *Proposal for a Regulation of the European Parliament and of the Council of 11 May 2022 Laying Down Rules to Prevent and Combat Child Sexual Abuse (COM(2022) 209 final).*

Riddell, A. (2013). "Evidence, Fact-Finding, and Experts", in *The Oxford Handbook of International Adjudication*, eds C. Romano, K. Alter, and Y. Shany (Oxford: Oxford University Press).

Rosenfeld, A., and Richardson, A. (2019). Explainability in human–agent systems. *Auton. Agent Multi Agent Syst.* 33, 673–705. doi: 10.1007/s10458-019-09408-y

Sarker, S., Chatterjee, S., Xiao, X., and Elbanna, A. (2019). The sociotechnical axis of cohesion for the IS discipline: its historical legacy and its continued relevance. *MIS Q.* 43, 695–719.

Sooriyakumaran, D., and Jegan, B. (2020). *Race, Technology and the Necropolitics of Border Militarism: Corporate Actors Profiting From Refugee and Migrant Abuse.* Vienna: OHCHR.

Staatscourant (2019). *Samenwerkingsafspraken Betreffende de Technische Voorziening TRIP (Travel information portal). Nr. 51586, 7* October *2019.*

Statewatch (2022). *EU Police Plans for the Future of Travel are for a Future With Even More Surveillance. Statewatch News.* Available online at: https://www.statewatch.org/news/2022/august/eu-police-plans-for-the-future-of-travel-are-for-a-future-with-even-more-surveillance/ (accessed August 14, 2022).

Stirn, B., and Bjorge, E. (2017). *Towards a European Public Law.* Oxford: Oxford Academic.

The Hague District Court. (2020). *SyRI legislation in breach of European Convention on Human Rights. ECLI:NL:RBDHA:2020:1878.* Available online at: https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBDHA:2020:1878 (accessed May 6, 2023).

Thönnes, C. (2022). *A Cautious Green Light for Technology-Driven Mass Surveillance.* Berlin: Verfassungsblog.

Thönnes, C., Salomon, S., and Guild, E. E. (2023). *The Future of the European Security Architecture: A Debate Series.* Berlin: Verfassungsblog.

Thönnes, C. N. (2023). *Automated Predictive Threat Detection After Ligue des Droits Humains.* Berlin: Verfassungsblog.

Tilburg University (2021). *Non-Discrimination by Design.* Tilburg: Tilburg University.

UNESCO (2023). *AI and the Rule of Law: Capacity Building for Judicial Systems. UNESCO.* Available online at: https://www.unesco.org/en/artificial-intelligence/rule-law/mooc-judges (accessed May 06, 2023).

United Nations (2021). *Gotravel Technical Introduction.* Available online at: https://www.un.org/cttravel/ru/goTravel (accessed May 6, 2023).

Varosanec, I. (2022). On the path to the future: mapping the notion of transparency in the EU regulatory framework for AI. *Int. Rev. Law Comput. Technol.* 36, 95–117. doi: 10.1080/13600869.2022.2060471

Wachter, S., Mittelstadt, B., and Russel, C. (2020). Why fairness cannot be automated: bridging the gap between EU non-discrimination law and AI. *Berkeley Technol. Law J.* 35, 3547922. doi: 10.2139/ssrn.3547922