Information Polity 27 (2022) 131–146
DOI 10.3233/IP-211531
IOS Press

The European PNR Directive as an instance of pre-emptive, risk-based algorithmic security and its implications for the regulatory framework

Elisa Orrù
Centre for Security and Society, Freiburg University, Werthmannstrasse 15, 79098 Freiburg, Germany
Tel.: +49 761 203 677 10; Fax: +49 761 203 677 95; E-mail: elisa.orru@philosophie.uni-freiburg.de

Abstract. The Passenger Name Record (PNR) Directive has introduced a pre-emptive, risk-based approach in the landscape of European databases and information exchange for security purposes. The article contributes to ongoing debates on algorithmic security and data-driven decision-making by fleshing out the specific way in which the EU PNR-based approach to security substantiates core characteristics of algorithmic regulation. The EU PNR framework appropriates data produced in the commercial sector for generating security-related behavioural predictions and does so in a way that gives rise to a paradoxical normativity directly dependent on empirical states. Its 'securitisation move' is moreover characterised by an inherent tendence to expand. As a result, the PNR Directive poses challenges for existing check and balance mechanisms and for human autonomy. These challenges could be partially addressed by strengthening *ex-post* control procedures and independent auditing. Yet in the decision to adopt a risk-based security model, something more fundamental seems to be at stake, namely, the preservation of the idea of human beings as moral agents able to direct and modify their behaviour in accordance with an intelligible, reliable and predictable normative order.

Keywords: Passenger Name Record, PNR, algorithmic regulation, algorithmic security, pre-emptive security, risk-based security, behavioural profiling, predictive behavioural analysis, securitisation

Key points for practitioners:

- The current European PNR framework creates challenges for traditional checks and balances that are at the core of democratic and rule-of-law systems.
- Pre-emptive, risk-based security approaches have an inherent tendency to facilitate the expansion of surveillance opportunities and apparatuses.
- There is a need for improved safeguards whenever pre-emptive security measures are adopted. Improvements should focus on strengthening reporting duties, enabling independent auditing and setting up control bodies with the capability to issue binding recmmendations. IT auditing techniques (e.g. black box methods, reverse engineering) can effectively support independent auditing.

1. Introduction

This article aims to contribute to the debate on 'algorithmic regulation' (Yeung, 2018) by enriching it with an analysis of Europe's Passenger Name Record (PNR) Directive. It draws on and brings together existing research in the interdisciplinary field of security studies focusing on 'algorithmic security' (Bellanova & de Goede, 2022, p. 102; Ulbricht, 2018) and legal scholarship on the implications of

1570-1255 © 2022 – The authors. Published by IOS Press. This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial License (CC BY-NC 4.0).

'data-driven' regulation for the rule of law (Hildebrandt, 2018; Bayamlıoğlu & Leenes, 2018). It does so from the standpoint of practical philosophy and, within this disciplinary field, adopting a critical realist approach. Critical realism is an emergent and interdisciplinary approach in practical (and especially political) philosophy which takes observed political, legal and social phenomena as starting points, rather than beginning with moral or otherwise normative principles (Geuss, 2008; Williams, 2005; Zolo, 1992; Rossi & Sleat, 2014). This approach does not renounce normativity, though: the analysis of existing phenomena serves to critically examine them, to highlight tensions and contradictions between them and the normative claims which legitimate political and legal measures and, finally, to suggest ways of resolving those tensions and contradictions (Orrù, 2021).

The PNR Directive constitutes a privileged object of analysis for a critical-realistic investigation of current shifts in the European approach to security and their normative implications. It was introduced in 2016 and obliges Member States to centrally collect, process and retain data of flight passengers provided by air carriers. In the landscape of intra-European information exchange, the PNR Directive constitutes the very first implementation of a systematic, pre-emptive, risk-based approach to security. This is likely the beginning of a trend which will expand in the upcoming years, for instance through the already established introduction of the European Travel Information and Authorization System (ETIAS), which will be operative starting in 2022, or through an extension of PNR regulations to the maritime sector.

By analysing the case of the PNR Directive, this paper aims to contribute to the Special Issue's debates by exploring the ethical and legal challenges of Information and Communication Technologies (ICTs) used in the context of security. Specifically, it aims to highlight the implications of exploiting data generated with the support of ICTs for security purposes and the way the use of ICTs mediates security practices. It also explores the regulatory safeguards and constraints needed to meet the ethical challenges raised by these security applications.

In accordance with the critical-realistic approach, this paper begins by presenting and analysing the state of the art of current European PNR norms against the backdrop of global trends toward the exploitation of PNR data for security purposes since 9/11 (Section 2). It then describes the core characteristics of the approach to security embodied by the European PNR framework and connects it with the ongoing debate on algorithmic regulation (Section 3). Section 4 highlights the normative tensions and the implications for the regulatory framework which emerge from the European PNR-based approach to security (Section 4). Finally, the paper discusses possible regulatory remedies for the challenges posed by this kind of security approach (Section 5).

2. State of the art of PNR regulations

2.1. International bilateral PNR agreements involving the European Union (EU) and global developments

The focus of this article is on the European PNR framework as it is established by Directive (EU) 2016/681. The previously existing extra-European legislation and PNR international agreements are thus not the specific focus of this analysis. However, a short overview of the international and global landscape of PNR regulation will help clarify and contextualise the EU case and especially the role of the EU as, at once, a 'norm-taker' (Argomaniz, 2009) and an active contributor to the current process leading to the emergence of a global PNR regime.

In the direct aftermath of 9/11, the United States (US) adopted the Aviation and Transportation Security Act, which obliged air carriers to provide US customs, border control and security authorities access to

the passengers' data contained in their booking and departure control systems for flights to and from the US (Wojnowska-Radzińska, 2021, p. 117). As an upshot of this US legislation, a transatlantic agreement with the EU was needed in order to regulate the transfer of data by European Air carriers. A first US-EU Agreement was signed in 2004, but was shortly after declared void by the Court of Justice of the European Union (CJEU) for relying on the wrong legal basis. A new version of the agreement was signed in 2007 between the EU and the US, but data protection concerns lead to the drafting of a new agreement that was finalised in 2011 and signed by the EU Parliament in 2012. This agreement, still in force, requires and regulates the transfer of PNR data from the EU to the US, but not vice versa.

In addition to the EU-US PNR treaty, the EU negotiated bilateral PNR agreements with Australia (signed in 2011) and Canada (signed in 2006 and re-negotiated in 2014). The agreement with Canada, however, has never entered into force. Indeed, based on an EU-Parliament request issued in 2014, the CJEU decided in 2017 that some of the agreement's norms conflicted with the EU's Charter of Fundamental Rights (CFR; CJEU, 2017; Carpanelli & Lazzerini, 2017; Tambou, 2018). Negotiations for additional PNR agreements were launched in 2015 and 2020 with Mexico and Japan respectively (EU Commission, 2015; Maruhashi, 2020).

The existence of international PNR agreements, particularly the EU-US agreement, was a driving motivation for creating a European PNR regulation (Argomaniz, 2009; Bigo et al., 2015; Boehm, 2011). Indeed, EU authorities themselves did not have automatically access to the PNR data transferred to the US (De Hert & Papakonstantinou, 2009, p. 369; Blasi Casagran, 2015). Once the EU PNR Directive regulation was in force, it in turn triggered reciprocity claims by third states and led to requests for further bilateral PNR agreements (EU Commission, 2020b, p. 49).

Recently, the use of PNR data has been at the core of regulations at the global level as well. In 2017 and 2019, the Security Council (SC) of the United Nations has passed two resolutions which oblige states to collect, retain and transfer PNR data.[1] Originally, the duty was limited to the purposes of combating terrorism, but it has subsequently been expanded to include organised crime. Following the SC Resolutions, the International Civil Aviation Organisation adopted international standards in 2020 for the use of PNR data with binding character (EU Commission, 2020b, pp. 6–7).

2.2. The EU PNR Directive

The first proposal to introduce a PNR regulatory framework in the EU dates back to 2007, with a proposal by the EU Commission for a PNR Council decision (EU Commission, 2007). The Commission's proposal, however, lost its validity, due to modifications in the legislative procedures introduced by 2009's Lisbon Treaty. In the same year, the Council urged the Commission to prepare a new proposal in accordance with the new legal framework (European Council, 2009). This was presented in 2011 and contained provisions modelled on the EU-US PNR agreement (EU Commission, 2011). The proposal met with criticism from the EU Parliament, who rejected it in 2013 and thus temporarily halted the regulatory plans for introducing a European PNR framework (EU Parliament, 2013).

Following the terrorist attacks in Paris in January 2015, however, the Commission's proposal was presented anew. In the mutated political climate, marked by a widespread sense of insecurity, the EU Parliament was more inclined to accept security measures restricting fundamental liberties than two years before (Bigo et al., 2015) and, in 2016, the EU PNR Directive was finally adopted.

[1] These are UN Security Council Resolutions 2396 (2017) and 2482 (2019).

The PNR Directive entered into force in May 2016. At present, all EU Member States except Denmark have implemented the Directive. Denmark, as a consequence of its opting-out of the measures in the 'Area of Freedom, Security and Justice', is not bound by the Directive, while the United Kingdom (UK) was bound by the Directive until 31 January 2020.[2] The UK, however, joined the EU PNR regime on the basis of a separate agreement and Denmark put in place national legislation establishing an EU-like PNR regime (CJEU Avocate Général, 2022, fn 60).

The directive introduces a pre-emptive, risk-based approach to security that is a novelty in the landscape of EU data exchange. Indeed, according to its own text, the specific innovation of the intended use of PNR data consists in enabling member states to identify individuals who are *potentially* involved in serious crimes or terrorist activities but whose involvement was *not previously known* or suspected (PNR Directive, Nr. 6 and 7).

To that end, EU member states must oblige air carriers operating extra-EU flights to transmit the data collected as part of the reservation and check-in process to a central national Passenger Information Unit (PIU) run by the LEAs (usually the national or federal police) of the EU state from which the flight departs or that of its destination. These data are analysed by the PIU and can be transmitted to the central units of other EU member states, to Europol and to third countries as well. According to the PNR Directive, the processing of these data is limited to the purposes of 'preventing, detecting, investigating and prosecuting terrorist offences and serious crime' (Art. 1). The collection and processing of PNR data is mandatory only for extra-EU flights, but member states have the option of extending it to EU-internal flights (Art. 2). All but one of the member states that have implemented the PNR Directive so far have taken this option (EU Commission, 2020a, p. 10).

The passengers' data transmitted by air carriers to the PIUs consist mostly of data that the carriers collect as part of their usual booking and check-in procedures. These data include name and contact information of the passenger, date of reservation and of planned travel, itinerary, travel agency, payment information, seat number and other seat information, complete baggage information, potential other persons travelling jointly with the passenger and a free-text field for entering 'general information' (Annex I of the PNR Directive).

National PIUs check the received information against European and international criminal databases, such as the Schengen Information System (SIS). Additionally, the PIUs analyse the data received based on risk criteria established by the PIU itself in order to assess the risk-level of *each* passenger. The risk criteria, which are treated as classified, may at any time be adapted in response to the PNR data processed (Art. 6, Nr. 2, lit. c). Passengers whose scores qualify them as high-risk, and who still qualify as such after a manual check of their data processing results, are selected for further examination (Art. 6).

2.3. First implementation report and pending ruling by the CJEU

Two years after the expiration of the deadline for member states to transpose the PNR Directive into national law, the EC published a review report in accord with the provisions of Article 19 of the PNR Directive (EU Commission, 2020a). For the purposes of this review report, member states were to provide the EC with yearly statistics (Art. 20 PNR Directive).

The Commission's evaluation of the first two years is positive. According to the report, the statistics provided by member states indicate that PNR data are a useful and effective means for investigating and

[2] https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32016L0681, last visit 29.01.2022, see also EU Commission, 2020a, p. 8.

prosecuting serious crimes and terrorism. However, the Commission itself relativises this assessment shortly after:

> [It] should be noted that the statistics provided to the Commission are not fully standardised and therefore not amenable to hard quantitative analysis. In a similar vein, it is also necessary to recall that in most investigations PNR data constitutes a tool, or a piece of evidence, among others, and that it is often not possible to isolate and quantify the results attributable specifically to the use of PNR alone. (EU Commission, 2020a, pp. 9–10)

Accordingly, the report does not provide critical quantitative data such as the total number of datasets transferred to the national units, the number of passengers that have undergone additional screenings, the number of successful arrests or the share of false positives and false negatives. An independent assessment of the effectiveness, necessity and proportionality of the use of PNR data so far is therefore not possible.

The necessity and proportionality of the PNR measures have been questioned in national court proceedings that have led to requests for preliminary rulings by the CJEU, submitted in 2019 by the Belgian Constitutional Court and in 2020 by a German local court. Most of the questions posed to the CJEU concern the compatibility of the uses of PNR data with Articles 7 (Respect for private and family life) and 8 (Protection of personal data) of the CFR (Belgian Constitutional Court, 2019; see also Roda, 2020).

On January 27th 2022, the Advocate General of the CJEU released his preliminary opinion on the case submitted by the Belgian Constitutional Court. According to it, specific provisions of the Directive, for instance the ones allowing for a generalised *retention* of non-anonymised data or the collection of 'general information', must be modified or are to be declared invalid. However, the collection and processing of passengers' data envisaged by the Directives are not as such considered to be incompatible with Art. 7 and 8 of the CFR. This applies, according to the Advocate General, also to the check against pre-defined criteria for classification into risk categories (CJEU, 2022; Thönnes, 2022).

3. Characteristics of the security model inaugurated by the EU-PNR Directive

3.1. The PNR Directive as an instance of 'algorithmic security'

In a recent article, Karen Yeung defined 'algorithmic regulation' as referring to

> decisionmaking systems that regulate a domain of activity in order to manage risk or alter behaviour through continual computational generation of knowledge by systematically collecting data [...] emitted directly from numerous dynamic components pertaining to the regulated environment in order to identify and, if necessary, automatically [or promptly] refine the system's operations to attain a pre-specified goal (2018, p. 505).

Yeung's conceptualisation has been discussed with reference to different application areas (Eyert et al., 2022; Festic, 2022; Busch & De Franceschi, 2021, Peeters & Schuilenburg, 2018), yet the exploration of the concept for 'critically interrogating' the use of algorithms in the security domain is still quite novel. Interestingly, existing literature explicitly connecting the debate on algorithmic regulation with security research often focuses on PNR measures. Lena Ulbricht (2018) used Yeung's conceptual framing to analyse the German parliamentary debates which led to German law's implementation of the PNR directive. Similarly, it is through the lenses of Yeung's conceptual framework that Bellanova and de Goede (2022) reflected on the transatlantic regulations between the EU and the US on the exchange of PNR data and the Terrorism Financing Tracking Program. The present article aims to continue this

research on 'algorithmic security' (Bellanova and de Goede, 2022, p. 102) by focussing on the specific European PNR framework as it was set up by the PNR Directive. It thus situates itself on a middle ground between Ulbricht's focus on national regulation, and Bellanova and de Goede's transatlantic scope.

The European PNR Directive, like the German and transatlantic PNR regulations, can be fruitfully understood as an instance of algorithmic regulation. Indeed, it aims to provide authorities support as they decide which individuals pose a sufficiently high risk to warrant closer analysis. The system's suggestions are based on 'knowledge' generated computationally through the analysis of the PNR data and aim to reach a broadly (and quite vaguely) pre-defined goal consisting in fighting terrorism and criminality. In the following, I will set out to explore the distinctive characteristics and implications of the European PNR mode of algorithmic regulation.

3.2. Pre-emption and behavioural profiling

According to Yeung, algorithmic regulation systems can be reactive or pre-emptive, depending on the use they make of existing data. While reactive systems are based on the analysis of historical data, pre-emptive systems assess historic data in order to infer predictions about future behaviour (Yeung, 2018, p. 509). The EU PNR system incorporates both reactive and pre-emptive elements. Indeed, it uses historic data to detect existing violations or relevant past behaviour (by checking against existing official databases), but also to predict future behaviour. The main innovation of the PNR Directive derives from this second characteristic and consists in the introduction of a pre-emptive, risk-based approach to intra-European information exchange for security purposes. In addition to being checked for compliance with pre-established and known rules (not travelling with fake documents, not having committed a crime in the past, etc.), passengers are now screened in order to obtain a probabilistic assessment of their future behaviour. This approach is based on the assumption that mundane travel-related information can provide indications of a traveller planning or being involved in criminal or terrorist activity.

Yeung (2018) has further suggested that algorithmic regulation can be understood as a form of 'surveillant-driven social sorting' (512 f.). This general characterisation fits the EU PNR framework. Bellanova and Duez (2012, p. 122) have noted, moreover, that the PNR setting entertains a 'symbiotic' relationship with commercial socio-technical assemblages. These observations can be further substantiated by analysing the distinctive way in which the EU PNR framework introduces economically-oriented social sorting practices into the security domain.

Although personal data have been employed for ICT-supported categorisations since the last decade of the 20th century at least (Gandy, 1993; Lyon, 2003), a critical change occurred at the turning of the millennium. Shoshana Zuboff (2019, 2015) provides an insightful description of this turn, which has gone hand in hand with the rise of a new economic system she calls 'surveillance capitalism'. This new economic logic relies on the appropriation of the raw, collateral data produced by internet users and their transformation into behavioural predictions (Zuboff, 2019, p. 74). The basic logic of the pre-emptive approach of the PNR Directive is symmetric to the basic functioning of the surveillance economy as described by Zuboff. In the same way as private companies appropriate the information surplus created by non-commercial activities for commercial purposes, the PNR system is based on the appropriation of the information surplus produced by law-abiding and fully legal activities (such as booking a flight ticket) for security purposes.

Take, for instance, a passenger who buys a flight ticket shortly in advance of a flight, pays it in cash instead of by credit card and checks luggage weighing 30 kg for a 3-day roundtrip. Such bits of information are provided by travellers in order to fly and processed by airlines in order to provide their

services as air carriers. Within the PNR framework, they are appropriated by public authorities and used for (secondary) security purposes. In this new context, they are assumed to provide assessments of potential criminal or terrorist activity or intent. Although the bits of information mentioned above depict fully legal behaviour, they can, in combination, lead to a person be selected for further scrutiny. Indeed, they can be interpreted as indicating unusual, illogic or 'abnormal' behaviour. Additionally, they may be associated with behavioural patterns attributed to persons involved in criminal or terrorist activities, who, for instance, purchase a roundtrip but do not intend to fly back and take therefore much more luggage than they would need for a short trip.[3]

3.3. Risk-based security and its paradoxical normativity

The pre-emptive approach embodied by the EU PNR framework is tightly intertwined with a risk-based approach. The affinity between risk-based and algorithmic regulation has been highlighted by Yeung (2018, p. 511), as well. On her view, algorithmic regulation can be seen as a form of prioritisation based on classification into risk-levels and aimed at providing decision-making support in the allocation of enforcement resources. As has been noted, risk-based rationalities have emerged in different areas of state action (economy, health, security) when the state gave up on addressing or resolving a given problem (poverty, diseases, criminality) and opted instead for 'managing' it by keeping it at an 'acceptable' level (Aradau & Van Munster, 2007, pp. 98–99). In the domain of criminal law, this attitude is linked to 'actuarial justice', an approach that accepts criminality as a social fact and aims at managing the risk deriving from criminality and avoiding the occurrence of single, specific criminal acts (Yeung, 2018, p. 512). Also this general characterisation of algorithmic regulation as connected to the 'management' of risk and crime can be specified and enriched by a specific analysis of the approach to managing risk and individual behaviour within the EU PNR framework.

Indeed, the pre-emptive, risk-based security model of the PNR Directive not only clearly departs from reactive approaches, which address past events only, but also differs significantly from typical preventative approaches, which aim to address the causes of a given phenomenon (criminality, terrorism etc.) and to tackle it in a structural manner. A pre-emptive approach is much more interested in correlations than in causes, and is much more focused on individuals than on structural conditions.

As we have seen, the behaviour potentially leading to a high-risk score typically does not consist in prohibited actions. Additionally, within the EU PNR framework, risk criteria are not publicly known, since, so the argument goes, publicity would make them useless by enabling potential criminals and terrorists to modify their behaviour in order not to match the criteria that lead to a high-risk classification (Ulbricht, 2018, p. 30).

This functioning has critical consequences on the way we understand the relationship between facts and norms and on the role of norms as providing orientation for individual behaviour. Indeed, the risk-based security approach of the PNR Directive seems to be indifferent towards prescriptions for conduct as 'external' and more or less stable sets of norms and seems to rely instead on a sort of flexible normativity immanent to the empirical data analysed. Its aspiration is neither to provide rules of behaviour, nor to re-educate or discipline subjects.[4] On the contrary, individuals should behave as 'naturally' as possible in

[3]The example is fictive but builds on the basis of the information on the risk indicators made publicly available during German court cases that have led to the request for preliminary ruling at the CJEU. See the Statement by the Gesellschaft für Freiheitsrechte, 'Stellungnahme zu den verbundenen Ersuchen um Vorabentscheidung C-148/20 bis C-150/20, Deutsche Lufthansa u.a.', which is available at https://freiheitsrechte.org/home/wp-content/uploads/2020/09/GFF-Stellungnahme-an-den-EuGH-zur-FluggastdatenspeicherungPNR-Richtlinie-2020.pdf (last visit 02/02/2022).

order for the system to provide accurate predictions. Far from dissuading criminals and terrorists from committing the planned actions (either because of the possible punishment if they transgress laws or because of the possible failure of their plans due to strict checks), these pre-emptive security measures presuppose that potential criminals and terrorists can be more effectively identified (and stopped) if everyone behaves without knowing what actions are considered to indicate a threat.

Yet, behaving 'naturally' or 'normally' does not ensure that individuals without criminal or terrorist intent will receive a low-risk score, if their behaviour deviates in ways considered to be relevant for risk-profiling from average or 'logical' behaviour. It is evident that the 'norm' here has nothing to do with external prescriptions of allowed or prohibited behaviour; rather, it simply coincides with the 'normality' immanent to the empirical data.

This is particularly evident whenever risk criteria are automatically generated. It is not clear whether such automatic generation of risk indicators (as an alternative to their 'manual' definition by LEAs) is already used with the PNR framework, but it is surely part of the risk-based security logic and part of the techniques currently developed as part of the medium- and long-term vision.[5] Principally, any kind of behaviour that can be automatically captured and codified into patterns (such as, say, the patterns followed and the time needed to select the purchased itinerary while booking a ticket, travellers' movement trajectories at border crossing areas, the time spent and the number of visits at the airport's toilets, and so on) can be analysed against automatically generated risk indicators. The systems can be calibrated to provide alerts on the top 0.1% of travellers whose behavioural patterns deviate from the 'standard' trajectories most significantly.

Even if the risk criteria are 'manually' set by humans and not automatically generated by machine intelligence, they can be meaningfully used only if they allow for the selection of a small group of travellers. Whether, for instance, paying by cash can be considered a risk indicator or not depends very much on the share of travellers that use other means of payment. If cash payment is the norm on a given route, then the criterion 'purchase by cash' becomes useless as a risk indicator. So, the value of a given criterion as a risk indicator, rather than being a socially or legally fixed characteristic of a given action (such as being forbidden or being potentially damaging to others), depends to a high degree on the empirical behaviour of other people in the same situation.

The risk-based logic of security emanating from the EU PNR framework thus consists in shifting the relationship between facts and norms towards a kind of normativity that is directly dependent on the empirical data processed. The norm is 'mobile' (Amoore, 2011, p. 31 and 2013, p. 66; Leese, 2014, p. 505) in the sense that the 'normality' according to which 'deviations' are defined is not given as a fixed standard; rather, it fluctuates. The 'mobile norm', or 'data-informed-code', as Mireille Hildebrandt has defined it (2018, p. 3), however, does not coincide with the overarching legal norms prohibiting criminality and terrorism and attaching sanctions to them. Rather, the paradoxical normativity of the PNR Directive opens up a space which differs from the legally normed space, which distinguishes acceptable

[4] This does not mean, however, that risk-assessment on the basis of non-publicly known criteria does not induce normalisation or chilling effects. On the contrary, the more obscure the criteria are, and the more diffuse the feeling of being under surveillance is, the higher the risk of normalisation and self-censorship (Hornung & Schnabel, 2009a, 2009b). On the subjectivation effects see also (Matzner, 2017).

[5] A hint of the long-term vision of risk-based security can be found in the IATA/ACI Smart Security programme (https://aci.aero/about-aci/priorities/security/smart-security/) as well as in the description and reports of EU-funded research and innovation projects such as FLYSEC (https://cordis.europa.eu/project/id/653879/reporting), XP-DITE (https://cordis.europa.eu/project/id/285311/reporting) and TRESSPASS (https://cordis.europa.eu/project/id/787120) (last visit – all – 02/02/2022). The mentioned opinion of the Advocate General of the CJEU states, however, that the processing of PNR data should not be carried out by means of artificial intelligence systems (CJEU, 2022, p. 3).

and prohibited behaviour and attaches sanctions to the latter. It locates itself in an intermediate space, the space of the setting of risk criteria, according to which behaviours are sorted and possibly 'flagged' as deserving closer inspection. The 'flag' shares this intermediate character, since it locates itself between a 'simple' recommendation and a sanction (Bellanova and de Goede, 2022, p. 105).

In this space, at the level of risk criteria, the normativity generated by pre-emptive security thus gives up even the *aspiration* to set norms that are independent of the empirical reality and refer to a more or less external and stable regulatory system. Its main intent is to detect deviations *within* the *Sein* (what is), independently of their relationship with a *Sollen* (what ought to be).

4. Implications for the regulatory framework

4.1. Algorithmic security and the rule of law

Algorithmic regulation, especially in the field of security, has far-reaching implications for the moral, social and legal principles which are highly valued in democratic societies committed to the rule-of-law. Legal scholars have focussed on data-driven decision-making's impact on the rule of law (Bayamlıoğlu & Leenes, 2018; Hildebrandt, 2018). In connection to the emerging European PNR framework, moreover, Matthias Leese (2014) has highlighted how profiling techniques undermine anti-discrimination safeguards, as well as the principles of proportionality, purpose limitation and accountability. Vagelis Papakonstantinou and Paul De Hert (2015) stressed the vagueness of profiling criteria and lamented the lack of provisions which might ensure effective redress mechanisms in a (at the time they wrote) draft version of the PNR Directive.

In the following sections, I aim to integrate these strains of the debate by highlighting two further kinds of implications for the rule of law deriving from the European PNR-based approach to security. The first of these is concerned with the self-expanding logic of pre-emptive security and its negative impacts on the effectiveness of check and balance mechanisms. The second refers to the impact of individual risk-assessment on legal certainty and individual autonomy.

4.2. Existing checks and balances in face of the self-expanding dynamic of pre-emptive security

The pre-emptive PNR logic, has been argued, equates to a securitisation move, according to which every kind of behaviour is susceptible to being captured and analysed for security purposes (Ulbricht, 2018, p. 156; Amoore & Raley, 2016). A look at the European PNR framework shows how this securitisation move, once set in motion, has an immanent tendency to reinforce and perpetuate itself.

First of all, because the aim of pre-emptive security is to identify 'unknown suspects', the focus of behavioural profiling cannot be restricted to selected categories of people; it must include the largest sectors of the population it feasibly can. Indeed, the PNR scheme is based on the collection and analysis of data of *all* air travellers. Each and every person booking a flight is categorised into a risk class based on data collected during the booking and check-in processes, even if most travellers are classified as low-risk in the end. Large amounts of data from people having no criminal or terrorist intent are also needed in order to derive a standard of 'normal' or 'average' behavioural patterns against which anomalies and outliers can be defined (or used as training material for the automatic generation of risk-criteria).

Moreover, currently there is a growing pressure towards the extension of the categories of PNR data beyond the ones commonly collected during booking and check-in, as well as towards the expansion of the risk-based security logic to further areas. This tendency contradicts the clear commitment, expressed

during the preparatory phase and in the PNR Directive, not to impose the collection of any additional data than the ones already collected for commercial purposes (EC, 2011, p. 11; PNR Directive, Nr. 8).

The first PNR review report provides interesting insights that illuminate a tendency towards the expansion of the quality and quantity of data collected and processed. It suggests, for instance, adding passengers' dates of birth to the compulsory information to be collected and transmitted to the PIUs and to extend the duty to transmit PNR data also to tour operators and travel agencies (EC, 2020a, pp. 10–11; EC, 2020b, p. 43). A possible further development mentioned in the EC Report regards the extension of the collection and use of PNR data beyond air traffic to include rail, ferry and bus transport (EC, 2020a, p. 10).

Pending the aforementioned CJEU decisions, the EC opted not to introduce any changes to the PNR framework at this junction (EC, 2020a, p. 12). Nevertheless, the potential developments mentioned in the review report are indicative of a mental shift from using the 'data exhaust' of information already available to the active and purposeful generation of additional data. This resembles the way in which collateral data exploited in the commercial sector started to be 'hunted aggressively and procured largely through surveillance' once they proved to be lucrative (Zuboff, 2019, p. 94).

The suggestions included in the first review also indicate what will be on the agenda if the CJEU decision leaves room for further developments, or if unexpected events will once more create a political climate favourable to the acceptance of extended surveillance measures. Especially the broadening to rail, ferry and bus traffic would entail an expansion of surveillance opportunities and apparatuses. Indeed, it would adapt these modes of transport to the booking and check-in procedures we are accustomed to for flying, including compulsory nominal reservation and pre-boarding checks. If the CJEU Decision will follow the AG Opinion, indeed, no significant and generalised limitations to the collection and processing of passengers' data are to be expected. Although the Opinion recommend to limit the generalised *retention* of data in a non-anonymised form, it indeed considers 'the transfer and the generalised and undifferentiated automated processing of PNR data [. . .] compatible with the fundamental rights to respect for private life and to the protection of personal data' (CJEU, 2022, p. 1).

A further crucial aspect of the self-expansive logic of risk-based security derives from the use of non-criminal data for security purposes. The non-criminal data on which the PNR framework relies for the risk-assessment consist largely in non-verified information. These data are not taken from official databases, verified by security operators or otherwise checked for accuracy, but are based largely on information provided by the travellers themselves, for instance when they book a ticket online. This means a potentially high level of inaccurate information entering the PNR database, a correspondingly high rate of mismatches with official databases (due for instance to errors in spelling, typos, etc.) and additional difficulties in drawing reliable results for the risk assessment. It is difficult to imagine how this inaccuracy could be counteracted if not by activating a verification spiral which intrudes more and more into further spheres of human activity. Examples of such verifications include required uploading of an ID card and biometric real-time online identification during the booking process in order to make sure that the ID card matches the traveller and the verification of phone contact details via real-time messages and calls. Such practices are already realities in commercial applications, and an uptake by the security domain seems to be a logical development along the path of risk-based security inspired by commercial practices.

The pre-emptive shift of security measures and their self-expansive character poses serious challenges for traditional check and balance mechanisms typical of the rule of law. On the one hand, *ex-ante* control mechanisms such as parliamentary authorisation are at risk of being trivialised. The pre-emptive logic postpones the justification of security measures to a future that is not verifiable. The problem which these

measures should solve are not present (an increase in criminality or terrorist activity) but are projected into the future (a possible terrorist attack, a possible smuggling of a big quantity of drugs). Thus, the justification of these measures and of their continue expansion is also projected into a possible future and can neither be verified nor invalidated. Reference to past empirical evidence can hardly be used for discussing the necessity and proportionality of the suggested measures. Moreover, being the justification of pre-emptive security measures built on the avoidance of single, exemplary criminal episodes and terrorist attacks, *ex-ante* checks can be easily circumvented under the pressure of particularly striking crimes or terrorist attacks, as was the case when the PNR Directive was passed by the EU parliament, after years of reluctance, following the Paris terrorist attacks.

On the other hand, traditional *ex-post* checks, such as judicial reviews, though still as important as parliamentary authorisations, are episodic and reactive by nature. Their activation is bound to high procedural thresholds and preconditions and therefore can take place only in select cases (TEU, Art. 19, TFEU 251–281). They risk becoming effective only years after a questionable measure has been implemented. This holds not only in the case of the pending CJEU decisions on the compatibility of the PNR Directive with fundamental rights, which, in the most optimistic case, will be taken six years after the directive's entry into force, but was also the case of the Data Retention Directive, which the CJEU declared to be incompatible with EU fundamental rights in 2014, eight years after its adoption.

4.3. Legal certainty and individual autonomy vs the paradoxical normativity of risk-based security

The existence of a relatively stable and known set of rules providing orientation for one's behaviour is a core characteristic of (modern European) normative systems. Since the political turn of the modern era that has equated legitimate power with power tamed by the rule of law, the principle of legal certainty has played a crucial normative role in constraining arbitrary power. Legal certainty, according to its general meaning, requires that 'the addressees of laws must know the law in order to be able to plan their actions in accordance with it' (Raitio, 2020).

Although the principle of legal certainty, on a strict, technical legal interpretation, applies specifically to criminal law and judicial decisions, it applies in its broader sense also to decision-making in the hybrid domain covered by the PNR framework, which, as discussed above, opens up a hybrid space of normativity and behavioural influence between border controls, mobility surveillance and more classical law enforcement measures.

Within this space, individuals are subject to decisions by public authorities (i.e. perform closer scrutiny, prevent from boarding the airplane or crossing the border) based on opaque criteria. The addressees of these measures and norms are not provided with elements to guide their own actions.

This lack of transparency poses a problem and a challenge for the rule of law itself, as has been stressed by Yeung (2018, p. 517) and Hildebrandt (2016). Additionally, it implies a fundamental shift not only in the way the relationship between the ruled and the rulers is constructed and reflected through the regulatory framework, but also in the way individuals as addressees of the norms are conceived.

Bayamlıoğlu and Leenes (2018) elaborated on a similar aspect with specific focus on algorithmic regulation in the judicial context. They see intelligibility, reliability and predictability of the normative order as the core constituents of the rule of law. In traditional 'code-driven' regulatory systems, these attributes of the normative order are realised through the 'normative force' of the law:

> Rules, principles, standards and in general 'norms' [. . .] inform individuals about their way of conduct, and explain the legal course of events in situations addressed by the Law. Law, hence, is a normative enterprise where the legislator consciously creates legal effects (institutional facts) that obtain when certain conditions are met (Bayamlıoğlu & Leenes, 2018, p. 305).

'Data-driven' (or 'algorithmic') regulatory measures instead reject this causal enterprise of (explicitly and transparently) connecting legal facts with legal consequences and thus lack the normative force which is characteristic of regulatory measures under the rule of law. For Bayamlıoğlu and Leenes (2018, p. 309) this lack is problematic, because it constitutes a blow to human autonomy and deprives individuals of their right to effectively contest decisions by public authorities which affect their lives. Bayamlıoğlu and Leenes are principally concerned with the ineffectiveness of redress measures. Although Art. 15 of the PNR Directive establishes that national supervisory authorities must deal with complaints by individuals, the opacity of the risk criteria (and possibly of the subsequent measures) negatively affects the effective exercise of complaint rights. Bayamlıoğlu and Leenes' observations, thus, seem to apply to the EU PNR regime as well.

However, in my view the demise of the causal enterprise of regulatory measures operated by the PNR Directive additionally poses a problem for individual autonomy in a more fundamental way. The European PNR framework, by using non-criminalistic, mundane behavioural data, negates the possibility for individuals to direct their own behaviour based on predictions of (legal or administrative) consequences. It thereby challenges the conception of individuals as moral agents who are able to modify their own behaviour by orienting their actions on the basis of general and abstract norms. This problem in relation to human autonomy emerges prior to the stage in which redress mechanisms can be activated, when individuals can challenge decisions and measures taken by authorities.

5. Possible regulatory modifications and the irreducible threat to human autonomy posed by risk-based security

As the previous analysis shows, the pre-emptive, risk-based security model instantiated by the EU PNR framework poses fundamental challenges to existing check and balance mechanisms and to the principle of legal certainty. Some of these challenges can, in my view, be addressed by supplementing existing control mechanisms and strengthening them in those respects that currently can be easily circumvented by pre-emptive security measures.

A first possible remedy consists in strengthening control mechanisms on a continuous and automatic basis. These would not take place punctually nor would they be triggered on request (as currently is the case with judicial review), but would by default operate throughout the lifecycle of a measure. Such mechanisms would enable verification of the necessity and proportionality of the introduced measures and should allow a continuation of the measures only if their effectiveness and respect of fundamental rights are confirmed by empirical evidence.

Such controls could be exercised by independent committees empowered to formulate binding decisions. In respect of the current limitations of parliamentary control, such committees would represent a corrective by performing *ex-post* the control functions that, due to the projection into the future of the justification of pre-emptive measures, can no longer be exercised *ex-ante*. Operating on a continuous and default basis instead of being activated upon specific requests, they would, moreover, contribute to filling in the temporal gap which currently exists between the entry into force of norms which potentially conflict with fundamental rights and their verification by the CJEU. The need to address this temporal gap is especially urgent due to the dynamic, flexible and innovative character of security measures adopting pre-emptive approaches. Additionally, addressing this would facilitate the review of measures which do not fulfil the procedural thresholds required for forwarding a ruling request to the CJEU.

For such committees to work properly, more stringent reporting and transparency duties could be placed upon member states and the EC. As we have seen, the first review report by the EC on the implementation

of the PNR measures does not provide the kind of critical data needed for an independent verification of the PNR framework's effectiveness and proportionality.

Currently, Art. 20 of the PNR Directive obliges States to conduct national statistics and transmit them to the Commission, including the total number of passengers whose data have been processed as well as the number of passengers who have been subjected to closer scrutiny to the EC. Remarkably, this article does not include false positive and false negative rates among the compulsory information to be provided, despite the critical importance of that information for assessing the effectiveness of the PNR measures. Additionally, there is no obligation for the EC to include the information provided by Member States in the review report to be issued according to Art. 19 of the PNR Directive.

A more stringent reporting regime would require, by contrast, that the EC provides statistics on false positives and false negative rates, as well as on the total number of passengers whose data have been processed by the PIUs. As far as possible, such statistics should be publicly accessible (as it is currently the case for the reports on the functioning of large EU databases such as the SIS II and the VIS) and, in any case, should allow for independent auditing. An important role in auditing could be played by IT techniques, including reverse engineering, counterfactual explanation techniques and black-box methods, in order to identify the factors that are likely to influence a given system's output and to assess whether the system's categorisations are potentially biased (Wachter et al., 2017; Zweig, 2019).

Moreover, currently no direct consequences follow from a negative assessment of the proportionality or effectiveness of the implemented measures. Moreover, the only body routinely enabled to formulate amendments proposals to the PNR Directive is the EC itself (Art. 19 PNR Directive). By contrast, in the case of a negative evaluation of the results, independent oversight committees should be able to temporarily suspend the given measures (for instance until a decision of the CJEU is available) or to formulate binding recommendations for reforming the normative framework.

These suggested modifications, however, are only able to address the challenges posed by the pre-emptive nature of security to traditional checks and balances. Its risk-based character seems to affect the principle of legal certainty and human autonomy in a more fundamental way. The option for a risk-based mode of security indeed seems to presuppose a renunciation of these principles as core elements of our normative systems. If they should still play a role in the relationship between the ruled and the rulers, and in the way the norm addressees are framed by regulatory measures, institutional mechanisms such as stronger redress possibilities for individuals will be of little help. Instead, the very aspiration to derive indications of terrorist or criminal intent from mundane, non-security-related behaviour seems incompatible with the ideal of the normative order as an enterprise of orientation and coordination of autonomous beings who can derive guidance for their behaviour from general, intelligible and predictable norms.

6. Conclusions

In this paper, I have explored the shift that the PNR Directive has introduced in EU security policy towards a risk-based, pre-emptive paradigm. My 'critical interrogation' of the PNR scheme has contributed to the ongoing debates on algorithmic security and data-driven regulations in four ways. First, it has specified the distinctive way in which social sorting practices borrowed from the commercial sector intersect security practices within the EU PNR, namely by appropriating the 'raw' collateral information produced by commercial practices to generate security-relevant behavioural predictions. Second, the paper has highlighted how the reliance on a 'mobile norm' within the PNR regime gives rise to a paradoxical normativity, which renounces even the aspiration to set relatively stable and external norms to guide

individual behaviour. This implies – and this is the third point – a departure from conceiving individuals as moral agents able to orient their behaviour according to a set of general and abstract norms. Finally, the 'securitisation move' of the EU PNR security logic has an inherent self-expanding logic that seems to remain unchallenged, it its substance, by the most recent regulatory developments including the CJEU Advocate General's opinion. While part of the challenges posed by the EU PNR pre-emptive logic to the regulatory framework could be addressed by strengthening control mechanisms on a continuous and automatic basis, its risk-based approach to security and human autonomy seem to be *aut aut* alternatives. If the PNR Directive is, as I argue, properly seen as a 'Trojan horse' introducing a risk-based approach to European security, there is an urgent need to discuss and decide which of the two alternatives shall shape the future of EU security policy.

Acknowledgments

I thank my colleagues at the Centre for Security and Society of the Freiburg University for their valuable feedback on a previous version of this paper. Additionally, the paper has benefited greatly from the feedback of the anonymous reviewers and of the Special Issue's guest editors.

References

Amoore, L. (2011. Data derivatives: On the emergence of a security risk calculus for our times. *Theory, Culture & Society*, *28*, 24–43.

Amoore, L. (2013). *The Politics of Possibility*. Durham: Duke University Press.

Amoore, L., & Raley, R. (2016). Securing with algorithms: Knowledge, decision, sovereignty. *Security Dialogue*, *48*(1), 3–10.

Aradau, C., & Van Munster, R. (2007). Governing Terrorism Through Risk: Taking Precautions, (un)Knowing the Future. *European Journal of International Relations*, *13*, 89–115.

Argomaniz, J. (2009). When the EU is the "Norm-taker": The passenger name records agreement and the EU's internalization of US border security norms. *Journal of European Integration*, *31*(1), 119–136.

Bayamlıoğlu, E., & Leenes, R. (2018). The 'rule of law' implications of data-driven decision-making: A techno-regulatory perspective. *Law, Innovation and Technology*, *10*, 295–313.

Belgian Constitutional Court (2019). Request for a preliminary ruling from the Cour constitutionnelle (Belgium) lodged on 31 October 2019 – Ligue des droits humains v Conseil des ministres (Case C-817/19).

Bellanova, R., & Duez, D. (2012). A different view on the "making" of European security: The EU passenger name record system as a socio-technical assemblage. *European Foreign Affairs Review*, *17*, 109–124.

Bellanova, R., & de Goede, M. (2022). The algorithmic regulation of security: An infrastructural perspective. *Regulation & Governance*, *16*(1), 102–118.

Bigo, D., Brouwer, E., Carrera, S., & Guild, E. (2015). The EU Counter-Terrorism Policy Responses to the Attacks in Paris: Towards an EU Security and Liberty Agenda, Paper No. 81, CESP.

Blasi Casagran, C. (2015). The future EU PNR system: Will passenger data be protected? *European Journal of Crime, Criminal Law and Criminal Justice*, *23*(3), 241–257.

Boehm, F. (2011). EU PNR: European Flight Passengers Under General Suspicion – The Envisaged European Model of Analyzing Flight Passenger Data. In Gutwirth, S., Poullet, Y., De Hert, P., Leenes, R. (eds), *Computers, Privacy and Data Protection: An Element of Choice*, Dordrecht: Springer, pp. 171–199.

Busch, C., & De Franceschi, A. (2021). *Algorithmic Regulation and Personalized Law. A Handbook*. München: Beck.

Carpanelli, E., & Lazzerini, N. (2017). PNR: Passenger Name Record, Problems Not Resolved? The EU PNR Conundrum After Opinion 1/15 of the CJEU. *Air and Space Law*, *42*, 377–402.

CJEU (2017). Press Release Nr.8 4/17, Opinion 1/15, 26.07.2017.

CJEU (2022). Press Release Nr. 19/22, Advocate General's Opinion in Case C-817/19, 27.01.2022.

CJEU Avocate Général (2022). Conclusions de l'Avocat Général M. Giovanni Pitruzzella, Affaire C-817/19, 27.01.2022.

De Hert, P., & Papakonstantinou, V. (2009). The PNR agreement and transatlantic anti-terrorism cooperation: No firm human rights framework on either side of the atlantic, *Common Market Law Review*, *46*(3), 885–919.

De Hert, P., & Papakonstantinou, V. (2015). Repeating the mistakes of the past will do little good for air passengers in the EU – the comeback of the EU PNR directive and a lawyer's duty to regulate profiling, *New Journal of European Criminal Law*, *6*(2), 160–165.
EC (2007). COM (2007) 654 final, 06.11.2007.
EC (2011). COM (2011) 32 final, 02.02.2011.
EC (2015). Joint statement: Beginning of negotiations between Mexico and the European Union on PNR data transmission, Mexico City, 14 July 2015.
EC (2020a). COM (2020) 305 final, 24.07.2020.
EC (2020b). SWD (2020) 128 final, 24.07.2020.
European Council (2009). Stockholm Programme, "An open and secure Europe serving and protecting citizens", Doc. 17024/09, 02.12.2009.
EU Parliament (2013). Doc. A7-0150/2013, 29.04.2013.
Eyert, F., Irgmaier, F., & Ulbricht, L. (2022). Extending the framework of algorithmic regulation. The Uber case. *Regulation & Governance*, *16*(1), 23–44.
Festic, N. (2022). Same, same, but different! Qualitative evidence on how algorithmic selection applications govern different life domains. *Regulation & Governance*, *16*(1), 85–101.
Gandy, O.H. (1993). *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, Colo: Westview Press.
Geuss, R. (2008). *Philosophy and real politics*. Princeton: Princeton Univ. Press.
Hildebrandt, M. (2016). Law as information in the era of data-driven agency. *Modern Law Review*, *79*, 1–30.
Hildebrandt, M. (2018). Algorithmic regulation and the rule of law. *Philosophical Transactions of the Royal Society A*, *376*(2128). doi: 10.1098/rsta.2017.0355.
Hornung, G., & Schnabel, C. (2009a). Data protection in Germany I: The population census decision and the right to informational self-determination. *Computer Law & Security Review*, *25*, 84–88.
Hornung, G., & Schnabel, C. (2009b). Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention. *Computer Law & Security Review*, *25*, 115–122.
Krafft, T.D., Zweig, K.A., & König, P.D. (2022). How to regulate algorithmic decision-making: A framework of regulatory requirements for different applications. *Regulation & Governance*, *16*(1), 119–136.
Leese, M. (2014). The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. *Security Dialogue*, *45*, 494–511.
Lyon, D. (ed.) (2003). *Surveillance as social sorting: privacy, risk, and digital discrimination*. London: Routledge.
Maruhashi, T. (2020). Japan-EU Passenger Name Record Negotiations and Their Implications. In Kreps, D., Komukai, T., Gopal, T.V., Ishii, K. (eds), *Human-Centric Computing in a Data-Driven Society*, IFIP Advances in Information and Communication Technology, Cham: Springer International, pp. 100–114.
Matzner, T. (2017). Opening black boxes is not enough – data-based surveillance in discipline and punish and today. *Foucault Studies*, *23*, 27–45.
Orrù, E. (2021). *Legitimität, Sicherheit, Autonomie. Eine philosophische Analyse der EU-Sicherheitspolitik im Kontext der Digitalisierung*, Baden-Baden: Nomos.
Raitio, J. (2020). Legal Certainty. In Sellers, M., Kirste, S. (eds), *Encyclopedia of the Philosophy of Law and Social Philosophy*, Dordrecht: Springer. doi: 10.1007/978-94-007-6730-0_136-2.
Roda, S. (2020). Shortcomings of the Passenger Name Record Directive in Light of Opinion 1/15 of the Court of Justice of the European Union. *European Data Protection Law Review*, *6*, 66–83.
Rossi, E., & Sleat, M. (2014). Realism in normative political theory. *Philosophy Compass*, *9*, 689–701.
Tambou, O. (2018). Opinion 1/15 on the EU-Canada Passenger Name Record (PNR) Agreement: PNR Agreements Need to Be Compatible with EU Fundamental Rights. *European Foreign Affairs Review*, *23*(2), 187–202.
Thönnes, C. (2022). A cautious green light for technology-driven mass surveillance: The Advocate General's Opinion on the PNR Directive, VerfBlog, 2022/1/28. https://verfassungsblog.de/green-light/.
Ulbricht, L. (2018). When Big Data Meet Securitization. Algorithmic Regulation with Passenger Name Records. *European Journal for Security Research*, *3*, 139–161.
Williams, B. (2005). *In the Beginning Was the Deed, Realism and Moralism in Political Argument*. Princeton: Princeton University Press.
Wojnowska-Radzińska, J. (2021). Legitimizing pre-emptive data surveillance under the EU law: The case of the PNR Directive. *Ruch Prawniczy, Ekonomiczny I Socjologiczny*, *83*(1), 115–127.
Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, *12*(4), 505–523.
Zolo, D. (1992). *Democracy and Complexity: A Realist Approach*. Pennsylvania: Pennsylvania State University Press.
Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York: Public Affairs.
Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*, 75–89.

Author bibliography

Elisa Orrù is currently Associate Professor in Philosophy at the Freiburg University. In January 2020 she received her *Habilitation* (German qualification for full professorships) for the discipline Philosophy with a work on the legitimacy of digital security measures of the European Union.

She studied philosophy at the University of Milan (Italy) and completed a PhD in law at the University of Pisa (Italy) under the supervision of Prof. Danilo Zolo. As PhD candidate and, then, as postdoctoral fellow she has conducted research, among others, at the Husserl Archive in Freiburg (Germany), at the Max-Planck Institute for Criminal Law in Freiburg (Germany), and at Princeton University (New Jersey, USA).

She led the Freiburg research contribution to the EU H2020 project TRESSPASS on ethical issues of digital and AI-supported border controls, and currently is ethics advisor of the ERC Project EXTREME and the H2020 Project CIVILnEXT. She is member of several scientific committees and has served as expert reviewer, among others, for the European Commission (H2020 Programme) and for the German Research Foundation (DFG).