A cautious green light for technology-driven mass surveillance

Christian Thönnes 2022-01-28T14:18:09

Yesterday, on 27 January 2022, Advocate General (AG) Pitruzzella published his Opinion ("OP") in the Court of Justice of the European Union's (CJEU) preliminary ruling procedure C-817/19. The questions in this case pertain to Directive (EU) 2016/681 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 (in short: PNR Directive) and its compatibility with EU primary law.

In his Opinion (which, besides the Press Release ("PR"), was only available in French at the time of writing), the AG, while criticizing the PNR Directive's overbroad data retention period and its lack of clarity and precision in certain points, generally considers the PNR Directive to be "compatible with the fundamental rights to respect for private life and to the protection of personal data" (PR). His arguments are not convincing.

Certainly, much more can and will be written about this case in general and the Opinion in particular. This entry can only shine a light on some of the AG's major arguments. In so doing, it shall point out why, in my opinion, the CJEU would do well not to follow the AG's recommendations. Instead, I believe the PNR Directive is incompatible with Articles 7 and 8 of the EU Charter of Fundamental Rights (CFR). Consequently, it ought to be invalidated.

What the AG has to say about the PNR Directive

The PNR Directive obliges EU Member States to require air carriers to transmit a set of data for each passenger to national security authorities, where they are subjected to automated processing against pre-existing databases (Art. 6 § 3 letter a) and "pre-determined criteria" (Art. 6 § 3 letter b), which contain (allegedly) suspicious flight behaviors (such as a mismatch between luggage and length of stay and destination, see the Commission's Evaluation Report, point 5.1, in order to identify potential perpetrators of serious crimes or acts of terrorism (a more detailed description of the Directive's workings can be found in paras 9-18 of the AG's Opinion or here).

The AG points to certain (limited) problems with the Directive's wording. Firstly, he contends that point 12 of Annex I, enabling "General Remarks" to be included in PNR data sets, fail to "satisfy the conditions of clarity and precision laid down by the Charter" (PR, also para 150 OP). He also considers the Directive's five-year-retention period for PNR data excessive and proposes that this period be limited to cases where "a connection is established, on the basis of objective criteria, between those data and the fight against terrorism or serious crime" (PR, also para 245 OP). In addition, he provides clarifying criteria for the relevancy of databases under Art. 6

§ 3 letter a (para 219 OP), regarding the applicability of the GDPR (para 53 OP) as well as collisions with the Schengen Borders Code (para 283 OP). He also demands that, due to their lack of transparency, (at least some) “machine-learning artificial intelligence systems” (PR), should not be used for pre-determined criteria (para 228 OP).

The most resounding message of his Opinion, however, is that the PNR Directive’s mass retention and processing regime is “relevant, adequate and not excessive in relation to the objectives pursued” (PR) and thus compatible with Articles 7 and 8 CFR. He therefore recommends to let it stand, albeit with some interpretative limitations (para 254 OP).

Incompatibility with *Digital Rights Ireland* and its successors

The AG’s reasoning in support of the PNR Directive’s proportionality relies on his central finding that “the Court’s case-law on data retention and access in the electronic communications sector is not transposable to the system laid down by the PNR Directive” (PR). He is referring to decisions like *Digital Rights Ireland, Tele2 Sverige* and *Quadrature du Net*, in which the CJEU had laid down strict limits on governments’ power to collect and process telecommunications data. Notably, it posited that “the fight against serious crime […] and terrorism […] cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight” (*Tele2 Sverige*, para 103; also *Digital Rights Ireland,* para 51). Instead, the CJEU required that in order to be considered “limited to what is strictly necessary […] the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued” (*Tele2 Sverige*, para 110).

Evidently, the PNR Directive would clash with these criteria – were they found to be applicable. The collection and automated processing of PNR data is completely indiscriminate. Given Member States’ universal extension to EU domestic flights, it affects all European flight passengers, regardless of their personal histories and independently of a potential increased domestic threat situation (this is proposed as a possible criterion in *Quadrature du Net*, para 168). The use of pre-determined criteria is not, like the comparison against existing databases, aimed at recognizing known suspects, but at conjuring up new suspicions (see EU Commission PNR Directive Proposal, SEC(2011) 132, p. 12). Also, taking a flight is a perfectly ordinary form of human behavior. There is no empirically demonstrated connection to the perpetration of serious crimes or acts of terrorism (in para 203, the AG presupposes such a “*lien objectif*” without providing any evidence exceeding anecdotal intuitions about terrorism and human trafficking) and the PNR Directive, given its broad catalogue of targeted crimes, is not limited to dangers caused by air traffic. What behavior will be targeted next? Visiting the museum? Going to a rock concert? Belgium, for example, has already expanded the PNR Directive’s scope

to international trains, busses and ferries (Doc. parl., Chambre, 20152016, DOC 54-2069/001, p.7).

Good reasons for applicability

It thus is quite clear: Should *Digital Rights Ireland* and its successors apply, the PNR Directive is in trouble. Now, why wouldn't their criteria be transposable? The AG's arguments mainly turn on a perceived difference in sensitivity of PNR data, compared to telecommunications meta-data. The latter, the AG explains, contain intimate information of users' private lives (para 195, 196), and almost uncontrollable in their scope and processing because everyone uses telecommunication (paras 196, 198). Moreover, because they are used for communication, telecommunications data, unlike PNR data, have an intrinsic connection to fundamental democratic freedoms (para 197). PNR data, on the other hand, he opines, are limited to a delineated life domain and narrower target groups because fewer people use planes than telecommunication (paras 196, 198).

Under closer examination, this comparison falls apart. Firstly, PNR data contain very sensitive information, too. As the CJEU has pointed out in his Opinion 1/15 regarding the once-envisaged EU-Canada PNR Agreement, "taken as a whole, the data may, inter alia, reveal a complete travel itinerary, travel habits, relationships existing between air passengers and the financial situation of air passengers, their dietary habits or state of health" (para 128). Unlike the AG (see para 195 in his Opinion), I can find no remarks in Opinion 1/15 that would relegate PNR data to a diminished place compared to telecommunications data. But secondly, and more importantly, the AG fails to consider other factors weighing on the severity of the PNR Directive's data processing when compared against the processing of Directive 2006/24/EC and its siblings: The method and breadth of processing and the locus of storage.

Only a small minority of telecommunication datasets, upon government requests in specific cases (see Articles 4 and 8 of Directive 2006/24/EC), underwent closer scrutiny, while the vast majority remained untouched. Under the PNR Directive, however, all passengers, without exception, are subjected to automated processing. In so doing, the comparison against pre-determined criteria, as the AG points out himself (para 228 OP), can be seen as inviting Member States to use self-learning algorithms to establish suspicious movement patterns. Other EU law statutes like Art. 22 GDPR or Art. 11 of Directive 2016/618, as well as comparable decisions by national constitutional courts (BVerfG, Beschluss des Ersten Senats vom 10. November 2020 – 1 BvR 3214/15 -, para 109) are inspired by an understanding that such automated processing methods greatly increase the severity of respective interferences with fundamental rights. Moreover, while telecommunications data were stored on telecommunication service providers' servers (to whom users had entrusted these data), PNR data are all transferred from air carriers to government entities and then stored there.

Hence, there are good reasons to assume that the data processing at hand causes even more severe interferences with Articles 7 and 8 CFR than Directive 2006/24/EC did. It thus follows, that the case law of *Digital Rights Ireland* should apply *a fortiori*.

An inaccurate conception of automated algorithmic profiling and base rate fallacy

There are other problems with the AG's reasoning; completely untangling all of them would exceed this space. Broadly speaking, however, the AG seems to underestimate the intrinsic pitfalls of unleashing predictive self-learning algorithms on datapools like these. The AG claims that the PNR Directive contains sufficient safeguards against false-positives and discriminatory results (para 176 OP).

Firstly, it is unclear what these safeguards are supposed to be. The Directive does not enunciate clear standards for human review. Secondly, even if there were more specific safeguards, it is hard to see how they could remedy the Directive's central inefficiency. That inefficiency does not reside in the text, it's in the math – and it's called 'base rate fallacy'. The Directive forces law enforcement to look for the needle in a haystack. Even if their algorithms were extremely accurate, false-positives would most likely exceed true-positives. Statistics provided by Member States showing extremely high false-positive rates support this observation. The Opinion barely even discusses false-positives as a problem (only in an aside in para 226 OP). Also, it is unclear how the antidiscrimination principle of Art. 6 § 4 is supposed to work. While the algorithms in question may be programmed in way to not process explicit data points on race, religion, health etc., indirect discrimination is a well-established problem of antidiscrimination law. Both humans and algorithms may just use the next-best proxy trait. (see for example *Tischbirek,* Artificial Intelligence and Discrimination).

Now, the AG attempts to circumvent these problems by reading the PNR Directive in a way that prohibits the use of self-learning algorithms (para 228 OP). But that interpretation, which is vaguely based on some "*système de garanties*" (para 228 OP), is both implausible – it lacks textual support and the pile of PNR data is amassed precisely to create a use case for AI at EU borders – and insufficient to alleviate this surveillance tool's inherent statistical inefficiency.

This cursory analysis sheds light on some of the AG's Opinion's shortcomings. It thus follows that the CJEU should deviate from Pitruzzella's recommendations. The PNR Directive, due to the severity of its effects and its inherent inefficiency in fulfilling its stated purpose, produces disproportionate interferences with Articles 7 and 8 CFR. It ought to be invalidated.

Between 2017 and 2021, the author worked for the German NGO "Gesellschaft für Freiheitsrechte", among other things, on a similar case (C-148/20 to C-150/20) directed against the PNR Directive.
