A Directive altered beyond recognition

Christian Thönnes 2022-06-23T11:43:07

On 21 June 2022, the Court of Justice of the European Union (CJEU) rendered its decision in the preliminary ruling procedure C-817/19. The fate of Directive (EU) 2016/681 of 27 April 2016 (in short: PNR Directive) was at stake. In its decision, the Court provided a set of interpretative limitations, thus curtailing some of the Directive's surveillance powers. Some of the Court's guidelines will almost certainly force Member States to adapt their transposition laws, foreseeably embroiling them in protracted legal battles. This does not change the fact that the PNR Directive survives – as a strange beast altered beyond recognition.

The Court had a chance to decisively answer one of the most crucial questions facing European security law: Is indiscriminate mass data retention for and the technology-induced analysis of ordinary human behavior compatible with fundamental rights? It instead opted for an enigmatic compromise creating a whole host of new questions. This blogpost shall sketch out what they are.

Limitations

The decision contains many limitations on the PNR data processing regime. Many of these limitations are inspired by the Court's Opinion 1/15 regarding the once-envisaged EU-Canada PNR Agreement – and some of them strike at the heart of the Directive (descriptions of the Directive's workings can be found here, here and in paras. 22-38 of the decision):

Firstly, there are numerous limitations around the Directive's scope of application. The Court restricts the scope of the information provided in PNR datasets as prescribed under points 5, 6, 8, 12 and 18 of Annex I (paras. 130-140). It also limits the range of targeted crimes, emphasizing that "although […] the objective of combating serious crime is capable of justifying the serious interference" with Articles 7 and 8 CFR, "the same is not true of the objective of combating criminality in general" (para 148). Consequently, the Court criticizes that Annex II contains crimes which are less likely to have the "requisite level of seriousness" (para. 150) since the definition of "serious crime" in Art. 3 § 9 only pertains to maximum, not minimum sentences (see para. 151). Member States are therefore responsible to "ensure […] that that system does not extend to offences that amount to ordinary crime" (para. 152).

The Court also severely curtails the scope of Art. 2 § 1 which expressly enables Member States to extend the PNR regime's scope from extra- to intra-EU flights. All Member States made use of this option – some, like Belgium, even extended the PNR system to other modes of transportation, like trains, busses and ferries (Doc. parl., Chambre, 20152016, DOC 54-2069/001, p.7). According to the Court, this indiscriminate extension is disproportionate and must be changed: The PNR regime,

the Court writes, may only be extended to all intra-EU flights indiscriminately in exceptional situations when there is “a terrorist threat which is shown to be genuine and present or foreseeable” (para. 171). In the absence of such a threat, Member States must limit themselves “to certain routes or travel patterns or to certain airports in respect of which there are indications that […] justify that application” (para. 174). This restriction is buttressed by the procedural requirement that “the decision providing for that application must be open to effective review, either by a court or by an independent administrative body whose decision is binding” (para. 172). These criteria are explicitly inspired by Court’s 2020 *Quadrature du Net* decision (see para. 168 of that decision) on the mass retention of electric communications data.

Secondly, the Court introduces guardrails for the automated comparison of PNR data against existing databases and pre-determined criteria under Art. 6 § 3 of the Directive: Paragraphs 182-192 clarify that “relevant” databases under Art. 6 § 3 letter a only refer to databases about persons or objects sought or under alert which are based on non-discriminatory factors and possess a relation to the fight against serious crimes with a link to the carriage of passengers by air.

But more importantly, the decision contains language aimed at limiting the use of self-learning algorithms for the development of pre-determined criteria under Art. 6 § 3 letter b. It makes explicit reference to paragraph 228 of the Advocate General’s Opinion and determines that the “pre-determined” nature of these criteria ought to imply that “that requirement precludes the use of artificial intelligence technology in self-learning systems (‘machine learning’), capable of modifying without human intervention or review the assessment process and […] the assessment criteria […] as well as the weighting of those criteria” (para. 194). The Court adds that “the opacity which characterises the way in which artificial intelligence technology works” might make it “impossible to understand the reason why a given program arrived at a positive match”, thus depriving data subjects of their right to an effective judicial remedy under Art. 47 CFR (para. 195). Moreover, paragraphs 202-213 emphasize that for the purposes of individual reviews of positive matches by non-automated means under Art. 6 § 5, Member States must establish “in a clear and precise manner, objective review criteria enabling its agents to verify” the match’s validity (para. 206). The Court also seems to introduce notification requirements in cases of positive matches, writing that upon finishing the relevant administrative procedure, affected persons must be enabled “to decide with full knowledge of the relevant facts whether or not to exercise his or her right to the judicial redress” (para. 210).

Thirdly, the Court restricts the retention period for PNR data for ordinary cases from five years (see Art. 12 § 1) to six months (para. 262), and clarifies that the subsequent processing of PNR data after arrival or departure is only acceptable if an independent body has established “objective evidence capable of giving rise to a reasonable suspicion that the person concerned is involved in one way or another in serious crime” (para. 220).

Open questions abound

At first glance, this seems fit to satisfy some of those who criticized the PNR regime for being excessive. The fact remains, however, that the Court upheld an instrument of indiscriminate surveillance – and upon closer examination, the decision reveals many open questions.

The first question boils down to: Why choose this route? Almost none of the Directive's central tenets have remained uncurtailed. The PNR Directive surviving this decision is very different from the one submitted for review. Some of the newly-introduced limitations lack any textual support. The notification requirement in paragraph 210 is completely absent in the Directive's text. So is any restriction on Member States' competence to extend the PNR regime to intra-EU flights in Art. 2 (contrary to para. 171). Art. 12 § 1 clearly states that the retention period for PNR data is five years, not six months (contrary to para. 262). In an introductory passage the Court emphasizes that "if the wording of secondary EU legislation is open to more than one interpretation, preference should be given to the interpretation which renders the provision consistent with primary law" (para. 86). It is also an established principle of EU law, however, that, at least for national law, valid interpretation ends where it would be *contra legem* (see for example the CJEU in *Mono Car Styling*, para. 61). It is hard to see why this would not apply to the conformity of EU secondary with primary law; if a secondary legal act does not contain language with criteria necessary for its compatibility with primary law, the Court shoud not invent it (see *Digital Rights Ireland*, paras. 65-71). This is not only a matter of democratic legitimacy. It will also be difficult for Member States to comply with the reformed PNR Directive without having any legislative text to lean on. I have stated elsewhere that, in my opinion, the Court should have invalidated the PNR Directive. Upon reading this decision, I was baffled to find that the Court seemed to share almost all of my concerns, yet declined to follow the law where it led.

Secondly, upon closer examination, some of the much-hailed limitations may turn out to overpromise and underdeliver. For example, the decision has been praised for containing a prohibition on the use of self-learning algorithms for surveillance purposes. Strictly speaking, this is not true. Paragraphs 194-195 contain prohibitions on self-learning algorithms which (1) are capable of modifying their assessment criteria without any human intervention of review (this notably open logical distinction does not matter much at the moment), and/or (2) are too opaque to allow for effective judicial remedy against their recommendations. This may cover most of today's available AI software. It is not inconceivable, however, that AI software could, in the future, provide satisfactory reasons for their recommendations (see for example *Wischmeyer,* Artificial Intelligence and Transparency: Opening the Black Box). Also, there are methods of supervised and reinforced learning where autonomous learning is intertwined with human interventions (see *Binns/Veale,* IDPL 11 (4), 319-332). Therefore, the prohibition on self-learning algorithms is a positive step forward – but without further legal elaboration security agencies could circumvent this prohibition if they just use the right AI systems.

The Court also calls upon Member States to come up with clear and precise criteria for objective review of automated matches (para. 206). It is unclear what they are supposed to be. I failed to find them in the decision. It is hard to conceive of any review criteria suitable to remedy the extreme rate of false-positives anyway. As stated before, because of base rate fallacy, this rate is a mathematical near-certainty – which is why the PNR system is and will be inefficient in combating serious crime.

Thirdly, is remains to be seen what this decision portends for the examination of future surveillance tools. For years, the Court's restrictive stance towards the mass retention of electronic communications data demonstrated in decisions like *Digital Rights Ireland*, *Tele2 Sverige* and *Quadrature du Net*, has seemed like a steady bulwark against surveillance scenarios. Notably, the Advocate General's Opinion heavily relied on his (in my opinion erroneous) claim that electronic communications data are unique and that therefore, the case law of Digital Rights Ireland ought not to apply to other types of data (see para. 199 of his Opinion). I can find no language in the PNR decision, where the Court expressly adopts the AG's position. It is conspicuous, however, that the Court is very quick to accept anecdotal evidence that the goals pursued by the PNR Directive "by their nature, have an objective link, even if only indirect one, with air travel" (para. 153), without citing *Digital Rights Ireland* or *Tele2 Sverige*. The decision contains no criteria decisively preventing further instruments of indiscriminate surveillance – the future relevance of *Digital Rights Ireland* therefore seems far from certain.

Dubious Consequences

It is hard to say what this decision will entail, both for the future of the PNR system itself, and the future of doctrinal EU security law as a whole. One of its products, however, seems to be further legal conflict.

Many of the restrictive interpretations introduced by this decision delegate very difficult practical and legal questions to Member States. Most national transposition laws contain provisions which quite evidently clash with a lot of these requirements. Member States will most likely be embroiled in protracted legal battles before national courts, litigating the conformity of their implementation laws with the at-times vague (sometimes even borderline-impractical) requirements of EU law under the PNR decision. The preliminary ruling procedure launched by the Administrative Court of Wiesbaden in a proceeding organized by the German NGO "Gesellschaft für Freiheitsrechte" (C-148/20 to C-150/20), for example, will likely shed some light on the compatibility of the German implementation law with the PNR decision.

Until these (very much justified) legal battles have been fought, there will be a period of significant legal uncertainty. This decision was evidently inspired by a willingness to strike a delicate balance between interests of security and freedom. This spirit of compromise is, in itself, laudable. I am not sure, however, if European security authorities would not have been better served with a clear decision to invalidate. Now, they will have to invest their scarce resources to come up with sophisticated review criteria for heaps of automatically generated data, the vast majority of which are absolutely useless, in order to combat an unspecified list of crimes occurring in

an unspecified group of locations – and they will be under close legal scrutiny along the way. Perhaps all of this will be a lesson to EU policy-makers: If you want to find needles, you should go look for them in smaller haystacks.

Disclosure: 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.
