Fundamental Rights at the Digital Border

ETIAS, the Right to Data Protection, and the CJEU's PNR judgment

Timo Zandstra & Evelien Brouwer

24.06.2022 doi: 10.17176/20220624-162402-0

Ever since the 1990s, the European Union has been constructing a vast digital infrastructure – including various information systems and databases – to expand the surveillance and control of the movement of third-country nationals. Today, we are witnessing the emergence of the EU's 'digital border': an ecosystem of interoperable databases, including SIS II, Eurodac, VIS, the EES, and the ECRIS-TCN, together with growing networks of screening rules and algorithmic risk assessment tools 'aimed at visualising, registering, mapping, monitoring and profiling mobile (sub)populations'. In this blog post, we discuss one of the latest additions to this ecosystem – the European Travel Information and Authorisation System, or ETIAS in short – and argue that the system as it is currently set up violates the right to data protection laid down in Article 8 of the Charter of Fundamental Rights, especially in light of the CJEU's PNR judgment earlier this week.

We are certainly not the *first* to suggest that ETIAS appears to be in violation of the right to data protection. But there are a number of reasons that make revisiting these arguments especially relevant today. First, ETIAS is the first 'smart' border system to use *algorithmic profiling* techniques to scan for 'risky' travellers. And in many ways, we consider ETIAS to be a test case for a much wider roll-out of such often AI-powered technologies in the field of border control. Keep in mind that the proposed AI Act contains a separate exception which excludes the use of AI in border control from the scope of its protective provisions. A second reason to revisit arguments to the effect that ETIAS violates the right to data protection is that ETIAS will be operational very soon, in May 2023. And a third, and more doctrinal, reason, is the CJEU's preliminary ruling of 21 June 2022 (C-817/19) in *Ligue des droits humains*. Finally, it is worth noting that the right to data protection is closely connected to other fundamental rights, such as the right to non-discrimination and to effective judicial protection.

Introducing ETIAS

ETIAS will comprise several elements. Its central system is set to collect and process personal data on *any* visa-exempt third-country national intending to travel to the EU, in order to predict whether they pose a 'security, illegal immigration or high epidemic (health)' risk, and to fill 'existing information gaps'. The ETIAS Regulation further introduces the new requirement that visa-exempt third-country nationals must obtain travel authorisation prior to departure, and sets up National Units which are to decide on that authorisation.

Under ETIAS, applicants for travel authorisation are to disclose a series of personal data – including those related to education and job group – through an online form. These applications for travel authorization are then automatically checked against all other relevant EU information systems, Europol data, and Interpol databases. The applicants' personal data will also automatically be checked against the new ETIAS watchlist – which is managed by Europol, Frontex, and Interpol – and against specific *risk indicators*, which are drafted under the auspices of the ETIAS Central Unit. Specific 'screening rules' which are to operationalise these 'risk indicators' will be 'built into an algorithm that will make it possible to identify travellers that fit pre-defined risk profiles'.

When this automated risk assessment triggers a hit, an ETIAS National Unit will manually decide on the application. Otherwise, travel authorization is granted automatically. If authorisation is granted, data

on ETIAS applicants entered into the ETIAS Central System will be retained for three years. If such authorisation is refused, annulled or revoked, the data will be held for five years.

The Right to Data Protection

As acknowledged in the recitals 29 and 41 of the ETIAS Regulation, ETIAS and its envisaged use interfere with the right to data protection as protected in Article 8 of the Charter. Whether it complies with the Charter thus turns on the question of whether this interference is justified in line with the requirements provided by Article 52(1) of the Charter, in particular the requirement of strict necessity.

On June 21st, the CJEU issued its first judgment regarding the requirement of strict necessity in the context of EU smart border systems in a preliminary ruling on the PNR Directive, which regulates the collection and processing of air passenger data. The Court held that the PNR Directive entails undeniably serious interferences with the rights guaranteed in Articles 7 and 8 of the Charter, insofar as, inter alia, it seeks to introduce a surveillance regime that is continuous, untargeted, and systematic, including the automated assessment of the personal data of everyone using air transport services.

In this judgment, the CJEU provides strict standards, making it clear that it is the obligation of the legislator to assess the *strict* necessity of the measure and to define a clear and *limited* purpose of the use of the personal data. Furthermore, the CJEU also limits the use of artificial intelligence technology in self-learning systems in the context of the advanced assessment of passengers on the basis of pre-determined criteria.

1. *Data collection and retention*

Already prior to its PNR judgment, the CJEU developed a series of important criteria to assess interferences with the right to private life and to data protection (Digital Rights Ireland, Tele2 Sverige, Quadrature du Net, Opinion 1/15 on the EU/Canada PNR Agreement). When applying the Court's criteria to ETIAS, it appears that, in the absence of an objective link, the indiscriminate collection of all visa-exempt travellers' data fails to meet the requirements of strict necessity. Even if all required data categories to be included in the ETIAS system are to prove effective, the necessity test further requires that they should also be *less intrusive* than other options for achieving that same goal. This cannot be established on the basis of the present Regulation, not least because its fails to adequately specify the purpose of including the various categories of data it requires.

In relation to data retention, the CJEU's recent PNR judgment moreover casts serious doubt on the viability of the three-year and five-year retention periods provided by the Regulation. According to the Court, after expiry of the initial retention period of six months, the retention of PNR data does not appear to be limited to what is strictly necessary in respect of those air passengers for which there is no objective evidence that would be capable of establishing a risk. This ruling is in line with the EDPS' concerns expressed over the duration of the retention periods in the ETIAS Regulation, and should recall the Commission's 2016 Feasibility Study's finding that "with time, the risk assessment performed after the application is submitted loses relevance as the person's situation may change". It is altogether unlikely that the Court's PNR ruling can leave ETIAS' retention periods unchanged.

It is really a missed opportunity, here, that the ETIAS Regulation has not been subject to a proper fundamental rights impact assessment. The Commission did not conduct an impact assessment of the Regulation in relation to the Proposal, nor did it organise a separate round of stakeholder consultations – even when the European Parliament's LIBE Committee, as well as the EDPS, *recommended* a targeted impact assessment.

1. *Prohibition on automated decision-making*

ETIAS' risk assessment procedure also appears subject to the safeguards which accompany the prohibition on automated decision-making laid down in Article 22 GDPR and Article 11 of the Law Enforcement Directive. These safeguards prescribe suitable measures which at

least include the right of the data subject to obtain human intervention on the part of the controller, and the right to obtain an explanation of the decision and to contest it.

It is relevant, here, that where ETIAS' risk assessment algorithm finds a 'hit', the application which generated that 'hit' will be processed manually by a National Unit (Article 26). This appears to constitute human intervention. But it is really unclear to what extent such human intervention will be meaningful in practice. In ETIAS, the human is 'looped in' at the end of the decision-making chain, where their judgment is already mediated by the 'risk score'. At this point, the promise of human judgment presumably unmediated by the socio-technical context within which it is embedded may well turn out to be an empty one. This is especially evident in the context of AI tools that are meant to 'help' National Units with their decision in case of a hit in the *automated* assessment, such as those that were already envisioned in a Deloitte study commissioned by the European Commission in 2020.

It is also unclear whether the grounds for refusal provided to the unsuccessful applicant enable that applicant to adequately contest the decision. Article 38(2)(c) of the ETIAS Regulation provides that the applicant is only entitled to the *category* of grounds for refusal (as listed under Article 37(1)). An applicant would then simply receive, for example, that they "pose a security risk". Without any further information concerning the reasons for that categorisation, it would be very difficult to adequately contest this decision – which appears to be exceedingly relevant for safeguarding the right to effective judicial protection as protected in Article 47 of the Charter as well. Here we may draw lessons from the CJEU's 2020 *R.N.N.S* judgment concerning the right to legal remedies against short term visa refusals. While the CJEU recognized the broad discretion of Member States in visa decisions, in order to ensure that the right to judicial protection is effective, the Court held that the person concerned must be able "to ascertain the reasons upon which the decision taken in relation to him or her is based, either by reading the decision itself, or by requesting and obtaining notification of those reasons".

What Now?

In light of these issues, we would like to propose a series of problems which, in our view, are central to the further development and roll-out of EU 'digital border' technologies, and of ETIAS in particular.

First, how can we ensure a *meaningful* human in the loop, especially where the human is 'looped in' at the end of the decision-making chain, where their judgment is already mediated by a 'risk score'? This week's ruling prescribed "clear and precise rules capable of providing guidance and support for the analysis carried out" which are to, in particular, "guarantee a uniform administrative practice [...] that observes the principle of non-discrimination". But what would such rules look like in practice?

Second, how detailed can and should the grounds for *rejection* be that the applicant receives, in order to meaningfully enable an appeal? Of course, there is a technical dimension to this problem. The algorithms might not be transparent enough to provide sufficiently detailed grounds (the so-called 'black box' problem). But there is also a strong normative dimension, as disclosing assessment frameworks might compromise national security (as well as, potentially, trade secrets).

A third problem concerns the politics around the use of (the term) AI. For example, when a group of researchers at the Université Libre de Bruxelles reached out to Frontex to request details concerning ETIAS' risk assessment algorithm, Frontex insisted that it would actually be more appropriate to talk about filtering queries than algorithms, and that no sophisticated analysis methods or any form of AI is involved in the risk assessment. This response is clearly at odds with a recent European Parliamentary Research Service report, which mentions ETIAS' screening algorithms as a prime example of a soon to be deployed AI tool, as well as the text of the Regulation (which defines the 'screening rules' as algorithms). But Frontex' response is paradigmatic for the politics around the use of AI in this space, as avoiding

this loaded term can serve to avoid additional scrutiny. And with the Court's PNR ruling that "[a]s regards [...] the advance assessment in the light of the pre-determined criteria, the [operating unit] may not use artificial intelligence technology [...] capable of modifying without human intervention [...] the assessment process and, in particular, the assessment criteria on which the result of the application of that process is based", we can expect to see more of it – as well as more pressure on the proposed exclusion of border technologies from the scope of the AI Act.

Different organizations and academics already called for amending the current Proposal for an AI Act to provide further safeguards with regard to the use of AI and large-scale databases in border and immigration decisions. In our view, it is clear that the EU legislator should also repair the current deficits with regard to the protection of fundamental rights and the use of the ETIAS system. New amendments to the ETIAS Regulation must provide sufficient safeguards and further limitations with regard to data processing and automated decision-making. There are two options to achieve this: either the EU legislator acts now, adopting legislative amendments before ETIAS becomes operational, or the CJEU will force the EU legislator to do so. Such a judgment can be triggered by preliminary questions and would be very important for further clarifying the contents of the strict necessity test in relation to 'smart' border systems, and for establishing the (un)constitutionality of the ETIAS Regulation in particular. It is worth noting, here, that the procedure which led to the preliminary ruling on the PNR agreement was initiated by Ligue des Droits Humain, a Belgian NGO. And it appears that the burden of policing the protection of fundamental rights at the EU's digital borders will for the time being remain with civil society.

ABOUT THE AUTHORS

Timo Zandstra
Timo Zandstra is an LLM student in Utrecht University's Legal Research Master.Timo Zandstra is an LLM student in Utrecht University's Legal Research Master.

Evelien Brouwer
Evelien Brouwer is a senior-lecturer in Public Law, Migration and Technology at Utrecht University and as researcher affiliated with the Montaigne Centre for the Rule of Law and Administration of Justice. Her areas of expertise include human rights and technologies, EU asylum and migration law, and access to justice.Evelien Brouwer is a senior-lecturer in Public Law, Migration and Technology at Utrecht University and as researcher affiliated with the Montaigne Centre for the Rule of Law and Administration of Justice. Her areas of expertise include human rights and technologies, EU asylum and migration law, and access to justice.

SUGGESTED CITATION

Zandstra, Timo; Brouwer, Evelien: Fundamental Rights at the Digital Border: ETIAS, the Right to Data Protection, and the CJEU's PNR judgment , Verfassungsblog, 24.06.2022, doi: 10.17176/20220624-162402-0.

Licensed under CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20220624-162402-0.