Caution: Safeguards may appear more robust than they are

Thorsten Wetzling 2023-05-09T14:09:43

When public authorities collect and process personal data, they interfere with people's fundamental rights and freedoms. For such interferences to be deemed lawful by European Courts, they need to be limited to what is necessary in a democratic society and subject to effective review by a court or an independent administrative body. So far, so clear. Yet, what does this mean in actual practice? European and national lawmakers often grapple with this question when they draft or amend security and surveillance legislation.

At a time when the European security architecture is evolving, and when national lawmakers must pay greater attention to an evolving set of common standards and safeguards to prevent disproportionate government access to data, it is essential to shed critical light on their implementation in actual practice. This post attempts to do this by examining the EU PNR Directive and the German legal framework on bulk collection. As different as these frameworks for untargeted surveillance are, they both include provisions that seek to prevent disproportionate government access and to ensure effective and independent review of data collection and subsequent data processing. This post tells a cautionary tale of good and less good attempts at meeting these important objectives by honing in on a few exemplary provisions and by discussing corresponding court findings thereon.

The good news

Lawmakers deciding over the general competence of public authorities to use untargeted surveillance instruments and the design of 21st-century oversight and accountability mechanisms can find a wealth of guidance in recent jurisprudence of the Court of Justice of the EU (CJEU) and the European Court of Human Rights (ECtHR), as well as landmark judgments by national courts. This evolving case law now provides a far more granular articulation of permissible objectives and common safeguards against executive overreach. In turn, this allows for clearer orientation and should facilitate lawmakers' delicate calibration of rights and interests.

Constant challenges

Caution is still needed, however, because the grown European repository does not prescribe specific practices. Rightly, this remains the responsibility of legislatures across Europe. When lawmakers take on the difficult task to refine and expand existing oversight and accountability mechanisms in accordance with the repository, the challenge remains that such mechanisms need to be adequately resourced, practised and (re-)evaluated. Else, practice on the ground stands no chance to

approximate the rules on the books. Furthermore, lawmakers enjoy substantial room for manoeuvre when implementing specific aspects of the repository. This, too, can bear several risks: As judgments typically proclaim only minimal standards, additional guardrails may be needed to ensure an independent and effective review of the use of fast-evolving technology. Moreover, lawmakers can avail themselves of too much *constructive ambiguity* in the drafting process: They might use vague language that, while conveying adherence to a certain safeguard, leaves practitioners too much leeway to pay only lip service to a particular requirement. As some examples discussed below show, a mere gestural implementation of the European repository runs counter to its overall objective.

Effective trimming of surveillance powers

Before turning to underwhelming practice, consider first the CJEU's review of the EU's PNR Directive, and recitals 183-188 of the judgment more specifically. It is where the CJEU sets an effective limit on the universe of databases that can be made available to Passenger Information Units (PIUs). According to Article 6 (3) (a) of the Directive, "the PIU may compare PNR data against databases relevant for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, including databases on persons or objects sought or under alert […]". The Court rightly identified a key problem of this provision: It does not specify which other databases could be considered 'relevant' in the light of the objectives mentioned. Given that Article 6 (3) (a) of the Directive does not expressly indicate the nature of the data that those databases may contain, or their relationship to the stated objective, the CJEU terminated this open-endedness to ensure that the PIU's access to personal data is not disproportionate. In so doing, it sets an effective limit as regards the amount of databases that PIU's can avail themselves for PNR comparisons: they can only use databases on persons or objectives sought or under alert (CJEU decision, paras 187-188). Without such exemplary trimming of this particular surveillance provision in the PNR Directive, the databases in question could have included a wide universe of information drawn from various collection methods, including but not limited to Open Source Intelligence and Social Media Intelligence. Rightly, the CJEU also addressed a grave concern and open question related to the management of such databases by private entities: They rarely are accountable to the same standards as public authorities.

Effective oversight empowerment

Another powerful advancement of the European repository occurred when the German Federal Constitutional Court (Bundesverfassungsgericht, hereafter BVerfG) decided in May 2020, that large tenets of the German foreign intelligence legislation were unconstitutional. This landmark judgement caused a major redesign and empowerment of intelligence oversight in Germany. Among the long list of deficits that the Court identified was an unduly strict interpretation by the German Government of the so-called third party rule. "[A]ccording to this rule, based on informal arrangements, intelligence obtained from foreign intelligence services may not be shared with third parties without the consent of the intelligence service in question" (BVerfG judgment para 293). The Court argued that independent and effective review of surveillance practices was too often torpedoed, or substantially

impaired, because of the untamed application of this rule in actual practice. Clarifying that the third party rule is "an administrative practice that is not legally binding, but is merely based on agreements with other intelligence services" (BVerfG judgment, para 294), the Court then held that "it is thus flexible and […] in the future, it must be ensured, through the way the oversight bodies are designed and through changes in agreements with foreign services, that the bodies conducting legal oversight are no longer considered "third parties" (Ibid).

In response to this judgment, the Bundestag created a powerful new judicial intelligence oversight body. It also had to make sure that it enjoyed comprehensive access to all premises, IT systems and operational databases of the foreign intelligence service and that "the Federal Intelligence Service cannot prevent oversight by invoking the third party rule" (BVerfG judgment para 85). As discussed in further detail below, this exemplary trimming of surveillance practice and bolstering of effective oversight should be born in mind when assessing decisions on legal frameworks, such as the PNR Directive, where important surveillance decisions are said to be "open to effective review by a court or independent administrative body" (CJEU decision, para 172).

Less effective safeguards against disproportionate government access to data

Yet, one can also find ample proof of less effective implementations of the growing European repository in actual practice. Consider, for example, the CJEU's findings regarding the "[s]afeguards surrounding the *automated processing of PNR data*" (CJEU judgment paras 202-213) and the rather vague documentation requirement of PIU activities this context.

Recurring to recital 7 and Articles 6(5) and (6) of the PNR Directive, the Court summarises that PIUs are required to:

- "define assessment criteria in a manner that keeps to a minimum the number of innocent people wrongly identified by the system established by the PNR directive";
- "individually review any positive match by non-automated means in order to identify to, as much as possible, any false positives";
- "carry out a review for the purpose of excluding any discriminatory results" (CJEU judgment paras 203).

Referring to "Article 6(5) and (6) of the PNR Directive, read in conjunction with recitals 20 and 22 thereof", the Court further underlines that Member States have important responsibilities regarding the implementation and review of these obligations. More specifically, they must:

- "lay down clear and precise rules capable of providing guidance and support for the analysis carried out by the agents" (CJEU judgment para 205);
- "ensure PIUs establish in a clear and precise manner objective review criteria enabling its agents to verify whether positive match concerns effectively individual who may be involved in terrorist offenses / serious crime, but also non-discriminatory nature of automated processing"; (Ibid., para 206) and

- "ensure that PIUs *maintain documentation* relating to all processing of PNR Data carried out in connection with the advance assessment" (Ibid., para 207).

Ill-defined documentation requirements invite creative non-compliance and prevent effective audits

Consider just the last point. The vagueness of the documentation requirement is striking. This should have been spelled out more specifically in the Directive, and, by extension, the Court. This is because some documentation practices are clearly more conducive to effective review by supervisory authorities than others. Vaguer documentation requirements constrain the supervisory authorities' access to relevant information. Put differently, they leave considerably more room for creative non-compliance by the PIUs. Hence it is important to know whether reviewers have comprehensive or only cursory access to the log files of the PIUs. Can they access this information directly or remotely? Depending on the answer to these questions, reviewers might benefit tremendously from automated control programs. In turn, this may significantly improve the ability of auditors to assess the legality and (provided their review mandate allows for it) the effectiveness of the data processing.

Unfortunately, the rather unspecified documentation requirement in the PNR Directive seems to have passed the CJEU's scrutiny. As a result, the documentation requirement seems more gestural in nature. For it to be an effective safeguard, there needs to be further mention of comprehensive access and investments and use of supervisory technology.

Merely "being open to effective review" is not enough

Another more gestural limitation of surveillance powers in the PNR Directive is tied to the way in which supervisory authorities are positioned to review the existence of a terrorist threat. Take situations where the signatories of the EU PNR Directive conclude "that there are sufficient solid grounds for considering that it is confronted with a terrorist threat that is shown to be genuine, present or foreseeable" (CJEU judgment, para 171). In such situations, according to the Court, Member States may decide, for a limited period of time, to apply the PNR Directive regime also to all intra-EU flights (Ibid., para 173). The CJEU stipulates, however, that this decision must be "open to effective review by a court or independent administrative body, whose decision is binding in order to verify that the situation exists, and that conditions and safeguards which must be laid down are observed" (Ibid., para 172).

This important safeguard may encounter significant difficulties when it comes to its implementation, however. For example, a review body may simply lack the competence, ability or resources necessary to independently "verify" whether a terrorist threat is shown to be genuine, present and foreseeable. Moreover, and tied to this, key information needed for this assessment may not originate from the Member State facing a terrorist threat. As previously discussed, supervisory authorities of a Member State may be prevented from seeing the data due to

national restrictions, for example unduly strict national interpretations of the ‘third party rule’.

Furthermore, an oversight body’s formal mandate may be limited to the assessment of the legality of a surveillance measure. Depending on national regulations, this may not include an independent verification whether the executive has sufficiently justified that a particular threat to the country is genuine, present and foreseeable. In addition, supervisory authorities across Europe have seen a remarkable increase in tasks that new legislation attributed to them. Apart from the necessary financial resources and technical equipment, supervisory authorities may simply lack the time or motivation to take on additional tasks. Thus, when planning new audits and inspections, some understandably tend to focus first and foremost on their formal remit. As a result of this, the mere fact the PNR Directive proclaims that important surveillance decisions are ‘open to effective review’ may not necessarily mean that they are going to be reviewed, let alone effectively.

Collusive delegation: The undesirable side effect of trimmed surveillance?

Let us revisit the German legal framework on foreign intelligence collection at the end of this cautionary tale. This will be done to caution against another potential form of accountability evasion that is likely to be found in other jurisdictions, too. More specifically, the ensuing discussion will show that the trimming of an agency’s surveillance powers will not prevent disproportionate processing of data if another, less regulated, agency is allowed to take over.

Reference is made to §24 (7) of the German BND Act. It embodies an important exception to the general restriction that content data may only be collected in bulk on the basis of search terms. Due to this exception, Germany’s foreign intelligence service may perform so-called *suitability tests*. This is done in order to test the suitability of specific telecommunication networks for bulk collection purposes or to generate new search terms or to assess the relevance of existing search terms. Some tests do not require a written order by the president of the BND and there is no requirement, as in other democracies, to involve independent oversight bodies in the process. Equally problematic, neither the duration nor the volume of the data collected in pursuit of suitability tests is subject to effective limitations. Even worse: According to §24 (7) of the BND Act, Germany’s foreign intelligence service may share an unrestricted amount of data it has collected in this way automatically with unspecified intelligence units within the German Armed Forces. Given that the various forms of *data processing* by the intelligence units of the German Armed Forces are nowhere near as strictly regulated, let alone independently overseen, this provision incentivizes what political scientists call collusive delegation. Agents who reportedly complain about an unduly restricted surveillance regime may rely on this provision to share more data with the Armed Forces not just because this is deemed necessary, but because its data processing is subject to fewer restrictions. This would clearly run counter to the European repository’s core objective and heeds a warning to lawmakers to adopt a functional or inter-agency approach when it comes to the implementation of the European repository. This, by the way, is also a central demand of the Council of Europe’s modernised Convention 108.

Conclusion

This post focused on a complex and ongoing challenge for many lawmakers across Europe: How to effectively implement the growing repository of European standards, norms and safeguards against disproportionate government access when amending or adopting new laws? The discussion shows that the risk of ineffective or gestural trimming of untargeted surveillance powers and ineffective review remains genuine. Yet, as the first two examples testify, there is also much progress and past mistakes are being rectified, too.

While ridding liberal regimes from illiberal practices requires constant work in progress, it is well worth the effort. It is what will distinguish the growing European security architecture from authoritarian regimes.
