

Squaring the triangle of fundamental rights concerns

Daniel Mügge

2023-05-12T14:32:39

Ex ante, the [July 2022 ruling](#) by the Court of Justice of the EU (CJEU) on Passenger Name Records (PNR) had a very specific scope — the use of passenger name records by government agencies. Upon closer inspection, however, it has important implications for the governance of algorithms more generally. That is true especially for the [proposed AI Act](#), which is currently working its way through the EU institutions. It highlights, ultimately, how national, or in this case European, legal orders may limit the scope for international regulatory harmonization and cooperation.

A potential clash with jurisprudential limits on AI policies

First of all, the PNR ruling, and the changes to the [PNR Directive](#) it implies, are a simple reminder that EU legislation is open to challenge in court. Obvious as it may seem, this consideration has hardly figured in debates about the AI Act. A wide range of stakeholders — including NGOs but also EU bodies such as the European Data Protection Supervisor—have voiced concerns about AI regulation plans. Those concerns frequently revolved around potential violations of ethical norms, for example, the right to privacy or non-discrimination. Most of these standpoints combined ethical arguments about what is desirable or not with technological arguments about the actual effects the application of certain algorithms would have. In contrast, few arguments considered whether certain AI use cases would even withstand legal scrutiny by the CJEU because they might violate fundamental rights, as outlined below.

This silence is remarkable. Many experts genuinely puzzle over when and where algorithms and fundamental rights may clash. And not only are there no easy answers: because of the speed with which AI technologies evolve, it is easily conceivable that legally contentious use cases emerge for which present-day law, and also a future AI Act, had not provided. (The haste with which [provisions about generative AI were inserted](#) into the negotiations at the 11th hour is instructive.) Sooner or later, legal challenges to the AI Act are to be expected, and it is anybody's guess how those will look, and how they will be decided.

The [PNR ruling](#) points to additional complications: one common discussion topic in AI debates is the explainability of algorithmic output, especially when algorithms are used in public policy decisions affecting individuals. Worries about discrimination also feature widely. At least with respect to the use of PNR in law enforcement and security contexts, however, the CJEU puts the bar even higher:

the [PNR Directive](#) itself requires that criteria for identifying subjects have to be “pre-determined” (§6.2(b)), and the Court finds that to be incompatible with self-learning algorithms [as long as the output is not transparent to humans](#). It thus turns the PNR Directive’s own wording against the use of algorithmic tools.

At the same time, in paragraph 195 of its ruling, it cites [Article 47 of the EU Charter of Fundamental Rights](#) — the right to an effective remedy — as potentially at odds with opaque and implicit selection criteria. This interpretation suggests that “unexplainable AI” might face much broader limitations in its applicability than only emanating from, in this case, the PNR Directive itself. After all, algorithms’ added value is to identify patterns in the data that humans would miss — self-learning algorithms are used precisely where criterium pre-definition fails. That may spell broader trouble for their use in public policy when potential fundamental rights are on the line.

Moreover, the ruling underlined the importance of proportionality: may potential rights-infringements be justified in light of the security risks that they tackle? Again, this question is thorny, because the potential uses of AI vary highly in the level of risks that they claim to address. Blanket rules for or against employing potentially rights-infringing AI in law enforcement seem difficult from that angle.

Irrespective of where one stands on these issues, the key is that there is significant scope for legal challenges of provisions in the AI Act. As the Schrems cases as well as the PNR ruling have shown, these kinds of challenges may be successful and can have momentous consequences. Up to now, there seems to be little realization that any compromises coming out of the AI Act trilogues might, at least in part, not withstand legal scrutiny, either now or in the future.

Extraterritorial implications

While a future AI regime for Europe is being negotiated, EU representatives have also been heavily involved in international talks and exchanges to craft AI rules. Those concern especially the OECD, whose [official AI definition](#) from 2019 [recently emerged](#) as a proposed compromise for the EU’s own legislation, and the Trade and Technology Council, the forum for transatlantic policy exchange and negotiation, which largely concentrates on digital technologies. Alignment of EU policy with international rules, and their embedding in a sort of transatlantic regulatory regime, are both important European policy goals. What does the PNR ruling imply for such efforts?

To begin, one reading of the CJEU’s decision is that, at least for certain use cases, EU citizens’ right to effective judicial remedies as spelled out in [Article 47 of the EU Charter of Fundamental Rights](#) is incompatible with algorithms whose results cannot be translated into clear criteria and are not certified discrimination-free. If so, that would generate hard limits on the AI-powered services and applications which non-EU companies could offer in the EU, either directly or indirectly. The AI Act may impose such limits on its own, as well. As an implication of the PNR ruling, or its juridical spirit, these limits would swing free from the will of legislators.

In other words, the fundamental rights of EU citizens, as interpreted by the CJEU, may define the outer boundaries of regulatory cooperation in the AI field — no matter how much goodwill there might be to find a compromise with, for example, the USA. Irrespective of whether these limits would be heeded in transatlantic or multilateral negotiations *ex ante*, or would emerge later on through successful legal challenges, as happened in the Schrems cases, they might cause serious frustrations among the EU's international partners.

This logic also casts its shadow on the outsourcing of rule-making to technocratic expert bodies, such as the [European Committee for Standardization](#) and the [European Electrotechnical Committee for Standardization](#) (see [Veale/Zuiderveen Borgesius 2021](#)), and potentially the [International Organization for Standardization](#) (ISO) and the [International Electrotechnical Commission](#) (IEC) as their global counterparts. Already, the relevant global standard setting committees ([subcommittee 42](#) of the ISO/IEC) ponder to what degree they would or should enter political or normative territory with their efforts, for example, to devise procedures to determine algorithmic bias. On the one hand, the CJEU's own interpretation of what would constitute a legally robust definition of such thorny concepts might compromise the formal independence of technical standard setters, given that fundamental rights would take precedence over any “technical” compromise the latter might devise. On the other hand, if such compromises were found to withstand legal scrutiny, they might offer an escape from otherwise fraught legal and ethical debates. Either way, the scope for outsourcing standard definitions that touch on fundamental rights questions would itself depend on the view of, and potential review by, the CJEU.

Finally, many aspects of AI technologies and their applications are bound to evolve significantly in the future. That includes the kind of data available to train them, technological ways to extract comprehensible “criteria” for (suggested) decisions from algorithms, and forms of applying them. As is the case generally, the legal framework for AI will therefore have to be dynamic in order to accommodate future technological and societal developments. This, too, limits the degree to which legislators or negotiators could lock the EU into particular bilateral or multilateral agreements on AI governance.

Future scenarios

If the PNR ruling implies that fundamental rights of EU citizens may demarcate the outer limits of EU-external regulatory cooperation, which scenarios does that suggest for the future? One scenario, somewhat surprisingly, is a form of inadvertent Brussels effect — but very different from Bradford's original logic ([Bradford 2020](#)). Here, other parties to regulatory negotiations might appreciate, however grudgingly, that certain safeguards in EU law may be unavoidable, no matter what they think of them — once more, the Schrems cases are instructive. The EU's limited room for manoeuvre on some of these questions may, in fact, strengthen its bargaining position.

It is equally plausible, however, that divergent regulatory preferences and unwillingness, or inability, to compromise might generate disparate levels of regulatory stringency even among, for example, the USA and the EU. If so, companies might “level up” to presumably higher EU standards voluntarily in the products they offer — a dynamic that [David Vogel \(1995\)](#) has dubbed the [California effect](#), in which American car producers voluntarily embraced stringent Californian environmental rules across their product palette. Alternatively, markets for AI-powered products might fragment to some degree, with more or less different versions of products on offer in different jurisdictions, each compliant with local laws. And, depending on how difficult it is to custom-tailor products to diverse regulatory regimes, some companies might opt to forego EU market access altogether, even if its overall market size is likely to mitigate against that approach.

In the meantime, the geopolitical climate has continued to deteriorate, not only in light of the Russian war against Ukraine, but also through souring Sino-American relations. AI governance, not least in the EU itself, had initially largely been framed as a technological, commercial and societal issue. Certainly, since the publication of the [report by the American National Security Commission on Artificial Intelligence](#), however, AI technologies are [increasingly viewed through a security and military lens](#). The EU AI Act itself steers clear of the intersection between AI and national security, not least in light of the EU’s limited competences there. To the degree that more and more aspects of AI governance were to be framed as security-relevant — for example, because of AI technologies’ dual use character — the scope of the AI Act provisions and the protections they provide might shrink. It will be interesting to see whether the CJEU, and its interpretation of fundamental rights, will then fill that gap and provide guardrails for AI development and application that at present are hardly considered.

The dilemma of fundamental rights, the need for legal flexibility, and international agreements

Taken together, algorithms may constitute a fundamental rights governance challenge, squeezing from three sides: first, fundamental rights as interpreted by the CJEU impose hard limits on what is and is not permissible. Second, at the same time, the speedy development of the technologies themselves would seem to call for a much more open-ended and flexible legal framework. And third, geopolitical as well as economic imperatives would seem to require the ability to commit to international agreements, irrespective of the former two considerations. The PNR ruling suggests how difficult that triangle will be to square, not only for passenger data, but for algorithms more generally.

