INTERNATIONAL JOURNAL OF SOCIAL SCIENCES BULLETIN
ISSN: (E) 3007-1917 (P) 3007-1909
Volume 4, Issue 3, 2026

FROM DIGITAL BORDERS TO DATA DIPLOMACY: EXTERNAL ACCESS TO EU BIOMETRIC MIGRATION DATABASES AND EUROPEAN DATA SOVEREIGNTY

Sajeel Ahmad[*1], Huda Binte Abbas[2]

[*1,2]*MPhil Scholars, Riphah International University, Islamabad*

[*1]sajeelhere@gmail.com

Corresponding Author: *
Sajeel Ahmad
DOI: https://doi.org/10.5281/zenodo.22198074

Received	Accepted	Published
26 January 2026	11 March 2026	25 March 2026

ABSTRACT

The EU has the most extensive system of biometric migration databases in the world-containing fingerprints and facial images of tens of millions of third-country nationals in Eurodac, the Visa Information System, the Schengen Information System, the Entry/Exit System, and their networked, interoperable sisters under the 2019 interoperability framework. What were initially purely internal measures for border and migration control are now increasingly becoming objects of third countries' externally driven access requests. This article maps the legal and institutional mechanisms by which third countries gain, or are attempting to gain, access to biometric data stored in, or emerging from, EU migration databases, and considers their implications for the EU's narrative of data sovereignty. Building on a qualitative research design utilizing doctrinal legal analysis and interpretive document analysis of secondary sources, I identify five mechanisms of access: transfer for returns purposes; urgent transfer for law enforcement purposes; a new Interpol interface mechanism; access through EU Agency-level operational agreements; and conditionality-driven mechanisms such as that envisioned in the EU-US Enhanced Border Security Partnership. I find that each mechanism undermined a pillar of EU data protection regulation: the adequacy mechanism, purpose limitation, reciprocity, or effective remedy. I argue that the source of eroding European data sovereignty lies less with external invasion than it does with internal abdication. The findings contribute to the literatures on digital sovereignty, fundamental rights, and the external dimension of EU migration management.

Keywords: *biometric data; data sovereignty; Eurodac; Entry/Exit System; third-country transfers; EU fundamental rights; interoperability*

1. Introduction

Twenty years ago, Broeders (2007) spoke of the nascent EU migration databases as "the new digital borders of Europe": a suite of information infrastructure for registering and rendering migrants legible to European states long before, and long after, they crossed a physical border. Today, that description understates things. Eurodac, which was originally conceived in 2003 for capturing the fingerprints of asylum seekers, has been recast as a powerful migration control mechanism under Regulation (EU) 2024/1358 that includes the capture of fingerprints and facial images of asylum applicants and irregular entries, those returned after search and rescue operations, and those granted temporary protection, and that mandates the recording of biometric data for children from the age of six. Regulation (EU) 2017/2226 added to this list the Entry/Exit System (EES), capturing the biometrics of almost all short-stay visitors to the Schengen area. European Travel Information and Authorisation System (ETIAS), mandated by Regulation (EU) 2018/1240, screens visa-exempt visitors against the EU's network of European and international watchlists. Overseeing this complex network is the

interoperability regulation of 2019, knitting together previously separate systems into one cohesive whole via an EU-wide search portal, a shared biometric matching service, a common identity repository, and a multiple identity detector.

The implications of this infrastructure for fundamental rights have been explored thoroughly and consistently, particularly the privacy dimension of rendering millions of third-country individuals searchable. What has received significantly less analytical scrutiny, both in scholarly writing and policy debates, is how this machinery is, and is intended to be, turned outwards towards other states. Who can access this system of biometric migration databases and under what conditions? What does it mean for the EU's much-heralded narrative of being a 'standard setter' for data protection, if external demands could turn this data trove into a tool that directly or indirectly serves the interests of non-member States? In recent years this question has gone from the niche corners of legal research to the center stage of EU policy and politics. Returns cooperation requires external sharing of identity data; ETIAS and the interoperability legislation connect EU screening systems directly to Interpol databases; Frontex operates within third countries on the basis of Status Agreements with personal data exchange mechanisms embedded within them; the United States has conditioned full visa waiver participation for all EU Member States' citizens on the conclusion of Enhanced Border Security Partnerships, containing provisions mandating "continuous and systematic" sharing of "biometric data" by December 31, 2026. The irony is difficult to miss. The EU prides itself, for valid reasons, on exporting its data protection regime on a global scale, what Bradford (2020) famously called the Brussels effect. At the same time, it currently maintains a biometrically driven surveillance apparatus over non-citizens unrivaled by democratic countries around the world, and is now facing increasing pressure to expose it to an increasingly diverse range of external partners. The critical test case for the notion of European data sovereignty lies in how the Union responds to this contradiction: can European data sovereignty be defined not as some abstract regulatory commitment protected by the Charter of Fundamental Rights, but merely as another piece on the bargaining table for mobility rights and migration cooperation? This article addresses three key research questions: First, through which legal and institutional arrangements do third countries gain, or propose to gain, access to third-country biometric data held in EU migration databases? Second, to what extent do these arrangements challenge core components of European data sovereignty? Third, to what extent do safeguards currently prevent these transfers from breaching EU fundamental rights standards, as confirmed by the Court of Justice of the European Union? The article proceeds by: reviewing the extant literature on digital borders, EU data protection, and digital sovereignty (section 2); setting out the relevant conceptual framework (section 3); describing the qualitative methodology employed (section 4); setting out the biometric migration database architecture (section 5); identifying and describing five data access mechanisms for third states (section 6); examining the challenges that these mechanisms pose to EU data sovereignty (section 7); and offering policy implications and concluding remarks (section 8).

2. Literature Review

2.1 Digital borders and the biometric turn

Numerous interdisciplinary readings have demonstrated how European border control has been transposed from a network of territorial checkpoints into an infrastructure of information. Amoore (2006) defines the phenomenon of 'biometric borders,' where the migrant body itself is the machine and the site of border inscription and invaded by the biometric data they carry, wherever they go. Broeders (2007) demonstrated how the conception of EU databases revolves around two mutually exclusive logics that make migrants undesirable for entry, namely, the expulsion of undesirables from the territory, and their recording, in order to facilitate their subsequent removal.

Bigo (2014) located expertise associated with command-posts of security in a specific professional universe, on par with border guards and navies, in opposition to the realm of border buses and ships, and that of cargo, as

one of the three professional worlds of EU border control, each with its own habits and spatial references.

Aas (2011) underscored how these systems produce a stratification, sorting out "crimmigrant bodies" from "banal travellers" and subjecting the latter to the most thorough surveilling gaze.

Recent literature has taken an infrastructural perspective. Dijstelbloem (2021) discusses borders as multilayered technopolitical infrastructures in which the politics are encoded in the design. Glouftsios (2021) details the bifurcated construction of information flows through the Visa Information System to illustrate how technical choices are political.

Trauttmansdorff and Felt (2023) narrate the digital transformation of the EU border regime as infrastructural experimentation, underpinned by a collective imagining of technology-as-control.

Leese (2022) interprets the creation of the interoperable framework as an effort to 'fix' state visions, synthesising apparently disparate data on third-country nationals into a single authoritative "truth." Bellanova and de Goede (2022) argue similar digital processes in security regulation. Collectively, the expansive existence of European migration databases has been revealed to be non-neutral, technologically embedded political projects. However, the body of work has been focused upon intra-European infrastructural life.

2.2 Data protection scholarship and the courts

The databases have withstood continuous fundamental rights challenges in the legal literature. As far back as 2008, Brouwer examined the serious practical obstacles to effective redress encountered by third-country nationals entered on the SIS. Boehm provided a charting of the structural mismatch between the sharing of information in the Area of Freedom, Security and Justice and the data protection principles purportedly governing it.

Tzanou theorised the intrinsic, independent relevance of a normative data protection fundamental right for counter-terrorism surveillance over and above privacy.

Vavoula provided an authoritative take on the migration databases themselves: in it she argued that the cumulative re-structuring of databases has created a generalised surveillance regime for mobile third-country nationals, incompatible with Articles 7 and 8 of the Charter. Quintel analysed the bifurcated applicability of the GDPR and LED to migration and security processing, thus documenting the gaps that leave third-country nationals 'floating between regimes'.

The EU Court of Justice has articulated the doctrinal yardsticks. In the famous Digital Rights Ireland, it struck down a general data retention directive for lack of proportionality. Opinion 1/15 found the proposed EU-Canada PNR agreement wanting due to its inadequate protection of sensitive data, its retention of data, and lack of independent oversight, in view of its obligation to comply with the Charter.

In Schrems II, the Court ruled that personal data can only transfer to countries affording 'essentially equivalent' protection to that within the EU, striking down the EU-US Privacy Shield for disproportionate US surveillance and effective redress issues.

The Ligue des droits humains ruling narrowed the applicability of PNR processing to only that information 'strictly necessary'. Together, these judgments seem to articulate a constitutional floor under the transfer of biometric data abroad. In 2018, the EDPS expressed a warning (which has more force once the stakes are external): 'The decision to establish interoperability is... A point of no return in the relationship between individual and the administrative state.'

2.3 Digital and data sovereignty

Another body of literature has addressed European digital sovereignty. Couture & Toupin (2019), for example, illustrate the fact that digital sovereignty is " a slippery signifier invoked for different purpose by states, indigenous groups and social movements. It has become one of the most contested signifiers of digital technology (so far)" while Floridi (2020) sees the struggles over digital sovereignty as a "conflict over command over data, software, standards and infrastructure" and characterises the EU as a unique actor attempting to achieve such control through regulation, while Christakis (2020), focuses on the tensions between the Brussels effect and Europe's

pursuit of strategic autonomy, highlighting the gap between sovereignty rhetoric and implementation.

Bradford (2020) notes how the EU projects rules outwards but does not shed light on situations where influence flows in the opposite direction, i.e.

When external powers demand access to European data. The present text can be located at the unexplored intersection of the three literatures. The data flows which emerge from the biometric migration apparatus, that is, which flow out of the apparatus, can illustrate something about what European digital sovereignty actually entails. This will link the internal debate overfundamental rights with the outward-looking contest over sovereignty, which have been developing in largely independent streams of thought.

3. Conceptual Framework: Data Sovereignty in Three Dimensions

Since 'data sovereignty' figures so prominently in policy discussions and is so loosely used, the article operationalizes it along three different axes. Normative control refers to the rules of access and transfer: whose rules apply to transfer-those of the EU in accordance with the principles of necessity, proportionality, and essential equivalence, or those of the receiving state? Operational control: who is able in practice to query, copy, or match the data-can EU authorities, within the EU, by way of a discrete, individual case, keystroke for keystroke, search for search, exercise control or must access be automated, systematic, and multilateral.

Accountability control: to whom are the data processors accountable-can supervisory authorities visit the flows, and can data subjects take their recourse in independent courts of law?

The polity has data sovereignty insofar as it exercises all three forms of control; it ceases to be a polity, not solely through outright surreptitious intrusion, but also through contracting arrangements that formally perpetuate control, while subverting it in fact.

A second check against a purely statist approach is to note that the data at stake is predominantly non-EU. It would be normatively inconsistent to maintain a conception of European data sovereignty that would regard only European data as belonging to the EU while the biometrics of third-country nationals could be mined for profit and traded in online markets (as we saw in the examples at the start of Section 1.2.2). As Articles 7 and 8 of the Charter protect 'everyone' and not only 'citizens,' this paper adopts a conception of data sovereignty based on human rights: sovereignty claims are justified if they underwrite Charter privacy and data protection standards to all data subjects. Ultimately, a human security approach recognizes that the individuals impacted by data sovereignty have a stake in it-it is important because it protects them, not just because it keeps foreigners out of the territory.

4. Methodology

A qualitative research design was used, integrating doctrinal legal analysis and interpretive document analysis; it relied solely on secondary and publicly accessible primary sources. The law permits doctrinal analysis used to delineate the EU legal framework-EU regulations and directives read in their entirety with focus on the relevant provisions regarding the communication of data to third countries and international organisations-which was interpreted in relation to Court of Justice (CJEU) case law. What is taking place politically: the use of interpretive document analysis to chart political developments in-Commission recommendations and proposals, Council documentation, statements and opinions from the EDPS and the EDPB, Fundamental Rights Agency (FRA) reports, and sustained observation of civil society groups, particularly Statewatch-whose leakage of Council documents has shed some light on EU-US negotiations.

Three classes of source materials constituted the research corpus. The first are primary legal documents, comprising the EU legislative proposals, and then founding and recast regulations of Eurodac, the EES, ETIAS, VIS, SIS, the two interoperability regulations, the GDPR and LED, and the European Border and Coast Guard Regulation. These legal bases were read and each relevant provision of each legal instrument relating to data access to persons/entities in third countries was

identified and then correlated with CJEU case law in doctrine.

Second are public institutional documents-which comprise institutional and supervisory documentation from 2018 to 2026.

Third are peer-reviewed academic articles-from 2006 to 2024 identified by systematic research into literature on migration studies, surveillance studies, and European law. For these articles, those directly relating to biometric databases, external data sharing, or digital sovereignty were selected. In the analysis, the documents were thematically coded with the classification of five external pathways as observed in Section 6 and four critical issues arising from the text as identified in Section 7. All data was triangulated so as not to depend unduly on one data source.

Three limitations may be highlighted. No interviews with officials in border agencies were carried out and hence current operational practices are not evident. Certain central negotiation documents appear to remain classified, implying that the EU-US perspective presented is, in part, dependent on leaked information and on reporting subject to unconfirmable omissions and/or to possible interpretations or manipulations.

The topic is, furthermore, evolving rapidly and so the account reflects the legal and political situation as it stood in the middle of 2026.

However, none of these limitations affects the strength of the doctrinal aspects of the argument: this relies on published law and case law.

5. The EU Biometric Database Ecosystem

To understand external access, one must first map out what exists. Six large-scale IT systems run by one centrally run agency (eu-LISA) collectively store and/or process biometric and biographic data of third-country nationals, with a seventh component to link them together. Table 1 shows the architecture.

Eurodac is the oldest component, and furthest from its origin. Originally set up to facilitate Dublin system allocation of responsibility through the comparison of fingerprints, its 2024 recast makes it into a general "migration management" database with facial images and fingerprints stored, the database applying to six-year-olds, persons rescued, beneficiaries of temporary protection, and including security flags, return decisions, and law enforcement access to Europol and national authorities (Regulation (EU) 2024/1358). The VIS stores every visa applicant's 10 fingerprints and photograph (Regulation (EC) No 767/2008).

The SIS alerts on persons including refusals of entry and return decisions; where available, the alerts also contain fingerprints, photographs, and (in the case of certain alerts) DNA profiles (Regulation (EU) 2018/1861).

The EES captures the fingerprints, facial photographs, and entry and exit dates of every third-country national present for stays of up to 90 days (or 5 years if they overstay) (Regulation (EU) 2017/2226). ETIAS itself does not store biometrics, but its checking logic reaches deeply into biometric databases; every application is automatically checked against the SIS, EES, VIS, Eurodac, Europol records, and two Interpol databases (SLTD, TDAWN) (Regulation (EU) 2018/1240, Arts. 12, 20). The ECRIS-TCN allows fingerprints and face images to be kept about convicted third-country nationals.

With the 2019 interoperability regulations, these silos of data transformed into an architecture. The European search portal (ESP) allows searching the systems and two Interpol databases with one search; the shared biometric matching service uses one algorithm to compare biometric data across the systems; the CIR aggregates data and the MID identifies potential identity fraud (Regulations (EU) 2019/817 and 2019/818). However, the EDPS (2018) warned that this process, by its nature, fundamentally alters the purpose of the databases, and the FRA (2018) showed how the processing of biometrics by the European Union at scale puts fundamental rights at risk due to potential error propagation and discriminate exposure.

Two features of this architecture are extremely pertinent.

The population of the systems is overwhelmingly non-citizens; these constitute an entire layer of surveillance built by Europeans on people from outside of the Union (Aas, 2011; Vavoula, 2022). In addition, because the systems can now share data, data that is stored in one system can now be used by another, so "data in" a certain file is actually

"data of" the entirety of these systems (Leese, 2022).

Table 1. EU large-scale IT systems processing third-country nationals' data and their external access dimensions.

System	Legal basis	Biometric data	Population covered	External access dimension
Eurodac	Reg. (EU) 2024/1358 (repealing Reg. 603/2013)	Fingerprints; facial images (from age 6)	Asylum applicants; irregular entrants; SAR disembarkations; temporary protection	General transfer ban with derogations for return cooperation; law enforcement access internally
VIS	Reg. (EC) No 767/2008 (as amended)	10 fingerprints; facial image	Short-stay visa applicants	Verification data may support return and readmission procedures
SIS	Regs. (EU) 2018/1860 to 1862	Fingerprints; photographs; DNA profiles in defined alerts	Persons subject to alerts, incl. entry bans and return decisions	No direct third-country access; indirect exposure via Interpol diffusion channels
EES	Reg. (EU) 2017/2226	Four fingerprints; facial image	All short-stay third-country nationals crossing external borders	Arts. 41 to 42: transfers for return and, exceptionally, law enforcement urgency
ETIAS	Reg. (EU) 2018/1240	None stored; queries biometric systems	Visa-exempt third-country nationals	Automated querying of Interpol SLTD and TDAWN databases
ECRIS-TCN	Reg. (EU) 2019/816	Fingerprints; facial images	Third-country nationals with criminal convictions in the EU	No direct external access
Interoperability layer (ESP, sBMS, CIR, MID)	Regs. (EU) 2019/817 and 2019/818	Consolidated biometric templates	All of the above	Single gateway through which Interpol databases are queried; magnifies reach of any access point

6. Pathways of Third-Country Access

The default principle throughout the rules governing the databases is ban: personal data held by the systems shall not be transferred or disclosed to any third country, international organisation, or private party. However, every ban is subject to exceptions, and a semi-shadow zone of operational and political compromises has emerged around the formal provisions. The study identified five different routes, presented in Table 2 and graphically represented in Figure 1. They vary by legal type, flow orientation, and volume, but all lead to

offshoring process identity to European screen or letting external actors in.

6.1 Return-related transfers

The oldest pathway applies to return and readmission. Article 41(1) and (2) EES Regulation, read together with Article 42, allows the transfer of identity data to a third country or an international organisation specified in Annex I, which includes UN organisations, IOM, ICRC, when it is necessary for the purpose of proving the identity of a third-country national for the purposes of return (Regulation (EU) 2017/2226).23 A new recast Eurodac Regulation retains the principle of the prohibition with the exception that data may be transferred to third countries as part of return cooperation procedures, under the provisions of Chapter V of the GDPR and domestic legislation pursuant to the LED, prohibiting them from revealing to the recipient third country the fact that the persons in question applied for international protection (Regulation (EU) 2024/1358).24 The latter safeguard is important as notifying an origin country of its nationals' search for protection may pose a risk for the person subject to persecution. The scholarly literature suggests, nevertheless, that the protection is often limited in practice, since even the very application for emergency travel documents to a deported person by a Member State might provide an indication of his/her prior movement patterns (Vavoula, 2022; Quintel, 2022). This pathway is case-driven and formally law-regulated but continues to rise with an increase in the European return policy volume.

6.2 Urgent law enforcement transfers

Further, there is a narrower channel that enables third countries' law enforcement authorities to gain access to EES data in urgent circumstances. Article 41(6) EES Regulation allows the designated authority "to transmit to a third country where an immediate threat to a terrorist offense or an immediate threat to life in connection with a serious crime exists" with certain preconditions: (a) where the transfer conforms to Chapter V of LED, (b) where a reasoned request is filed, and finally, (c) where the third countries concerned grant reciprocal access to their own entry and exit records to the Member States (Regulation (EU) 2017/2226, Art. 41(6)).

The conditions are cumulative, and the whole provision is obviously the exception rather than the rule.

Nevertheless, it is of analytical relevance for two reasons. First, it implicitly states reciprocity as the currency for the exchange of data and normalizes the idea that European biometric records can be 'traded'. Second, urgency-based deviations tend to become wider when subject to pressure (Boehm, 2012; Bigo, 2014).

6.3 Interpol interfaces

The third pathway runs in the opposite informational direction, but has structural implications. Every ETIAS application proactively interrogates the Interpol SLTD and TDAWN databases, and the interoperability framework makes those databases interrogable by the ESP, making available the alerts and diffusions stored in them; the regulation insists that the queries occur in such a way as to prevent the Interpol database owner from gaining knowledge that such a query has happened (Regulation (EU) 2018/1240, Art. 12; European Commission, 2021).

This architecture factor recognizes the real risk: Interpol's members are mostly authoritarian regimes that have a long history of abusing notices and diffusions even against activists, critics, and refugees.

It's precisely against this background that the EU sought a cooperation agreement with Interpol to secure protections and guarantees over such a database. However, even with a hit-not-reveal architecture, the pathway introduces the data of an external organization (including the governance failures thereof) into automated European decision-making about who should be allowed to travel. A wrongful SLTD or TDAWN notice filed by a repressive regime can result in a negative ETIAS decision. So here sovereignty is lost, not through data leaving Europe, but in decisions within Europe relying on data which Europe does not own (Leese, 2022; Vavoula, 2022).

6.4 Agency-level operational arrangements

Fourth, the institutional route: under Regulation (EU) 2019/1896, the border management teams provided by Frontex can be

deployed on the territory of third countries according to status agreements-which the Union has already entered into with West Balkan partners since 2019 with Albania, Montenegro, Serbia, North Macedonia, and Bosnia and Herzegovina, but most recently with other neighbouring countries as well. These agreements, along with the Frontex and Europol working arrangements, form the conduits through which operational personal data is exchanged between EU bodies and third countries' authorities, including especially identity and biometric data collected during joint operations. That the supervision of these data flows is notoriously fragmented-processing is taking place outside Union territory, under the responsibility of either the agencies or under the law of the host State-results in an accountability diffusion: where it becomes possible for any of the players to shift responsibility to the other as controller (Quintel 2022; Dijstelbloem 2021). For the data subject, typically the individual apprehended at an extra-EU border, the practical ability to invoke rights such as access to one's data, or correction or remedies, is nil (Brouwer 2008).

6.5 Conditionality-driven frameworks: the EU–US Enhanced Border Security Partnership

This fifth avenue has the most profound implications, and the most revealing implications. In February 2022, the US advised all participants to the VWP that continued visa-free travel would be dependent upon finalisation of an Enhanced Border Security Partnership (EBSP) with DHS, employing, in the phraseology used in descriptive literature and promotional materials, 'fully automated search and exchange of biometric and biographic data' (Statewatch, 2025; Council of the European Union, 2023). While some of the exchange activities involved in the PCSC agreements and the EU-US Umbrella Agreement focus on exchange related to terrorism and serious crime, EBSP provides for these data exchanges to occur on a constant basis, in the routine vetting of all arriving in a VWP member state. Washington has set December 31, 2026, as the absolute limit; if the Member States, on or after that date, have not yet negotiated an EBSP, their citizens will become subject to visa requirements (European Commission, 2025; Statewatch, 2026).

This avenue provides a live-time, up-close demonstration of the defense and erosion of data sovereignty. In Fall 2025, the Commission proposed that negotiations for a framework agreement authorizing such exchanges begin (European Commission, 2025), and in December 2025, the Council approved a negotiating mandate. There are two aspects of the mandate that need to be underscored: First, it explicitly provides that exchange shall not include direct use of centralized EU databases; data exchange will occur pursuant to bilateral agreements entered into, under the authority of the EU framework agreement, between the US and each member state from national repositories (Statewatch, 2025).

Second, the supervisors are forcefully inserted: the EDPS has warned that bulk biometrics-based immigration and border control checks performed by a third country set an important precedent for the future, and in March 2026, the EDPB Chairman wrote the Commission directly, citing concern regarding the ability of EU data subjects to exercise fundamental rights under US law, and regarding the retention of EU citizen data (Statewatch, 2026).

Exclusion from use of central systems is a genuine assertion of normative and operational control. Nevertheless, it can be seen to be porous as national databases now include fingerprints and facial images collected under relevant EU directives, the centrally stored SIS data will reside on national copies, and interoperability increases, blurring the lines between data in the central SIS repository and identical data in the Member States' repositories. Defense of data sovereignty at the level of eu-LISA's servers can be effectively bypassed at the Member State police repository level, and individual bilateralization of actual data streams fragments the Union's collective bargaining power and subjects individual members to direct US pressure (Statewatch, 2025; Christakis, 2020).

Table 2. Five pathways of third-country access and the data sovereignty tensions they generate.

Pathway	Legal or political mechanism	Direction and scale	Principal safeguards	Core sovereignty tension
P1. Return-related transfers	EES Arts. 41 to 42; Eurodac recast derogations; GDPR Ch. V	Outbound; case by case	Necessity for return; ban on disclosing asylum history; Annex I list of organisations	Identity data reaches states of origin where persecution risks may exist; inference risks despite formal safeguards
P2. Urgent law enforcement transfers	EES Art. 41(6); LED Ch. V	Outbound; exceptional	Cumulative urgency conditions; reasoned request; reciprocity of records	Reciprocity normalises bartering of biometric access; urgency clauses historically expand
P3. Interpol interfaces	ETIAS Art. 12; interoperability Regs.; envisaged EU–Interpol agreement	Inbound queries; systematic and automated	Hit-not-revealed query design; negotiated safeguards	European decisions depend on external records vulnerable to abuse by authoritarian members
P4. Agency arrangements	Frontex status agreements under Reg. (EU) 2019/1896; Europol arrangements	Bidirectional; operational	Agreement-specific data clauses; EDPS supervision of agencies	Accountability diffusion; data subjects effectively remediless in extraterritorial operations
P5. Conditionality frameworks (EBSP)	US VWP condition since 2022; EU framework mandate Dec. 2025; bilateral implementation	Bidirectional; continuous and systematic (proposed)	Exclusion of central EU databases; EDPS and EDPB scrutiny; Charter and Schrems II benchmarks	Mobility privileges traded against biometric access; bilateralisation fragments collective control

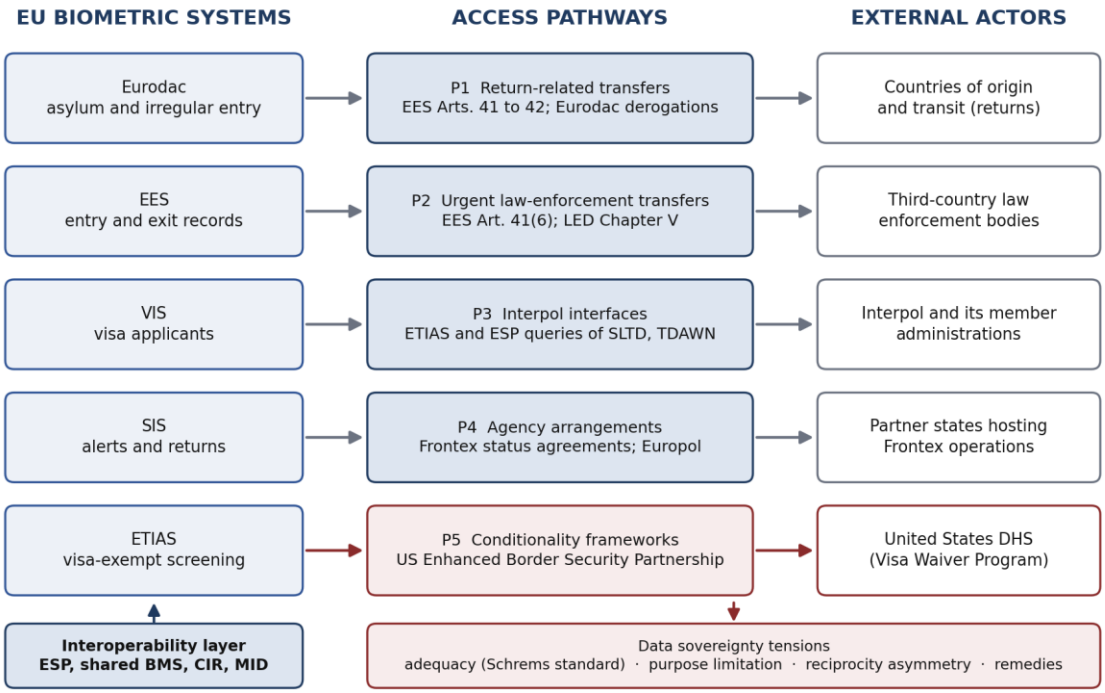

Figure 1. Conceptual map of third-country access pathways to EU biometric migration data and the resulting sovereignty tensions. Source: author's elaboration based on the legal instruments and documents analysed.

7. Challenges to European Data Sovereignty

7.1 The adequacy benchmark under strain

The first is doctrinal. While the GDPR and LED provide that transfers to third countries may only take place where there is an essentially equivalent standard of protection, whether via an adequacy decision, appropriate safeguards, or narrow interpretations of derogations (Regulation (EU) 2016/679; Directive (EU) 2016/680), Schrems II gave teeth to that requirement precisely with regard to the United States, whether considering the proportionality of surveillance law or the apparent lack of redress for Europeans (Case C-311/18, 2020). As Opinion 1/15 demonstrates, the Court applies the same strict scrutiny to security-focused agreements negotiated by the EU itself, invalidating clauses of the EU-Canada draft PNR agreement covering sensitive data and oversight functions (Opinion 1/15, 2017).

Continuous and systematic sharing of biometric data for immigration screening is a much more dynamic transfer than the passenger manifests involved in those rulings, and if the EBSP architecture does not secure enforceable rights, independent oversight, strict purpose use restrictions, and judicial remedies to all those impacted, it will suffer the same fate before the Court, and the EDPB's pointed questions over the Privacy Act and retention periods seem to indicate that the regulators are well aware of this (Statewatch, 2026).

The latter point is reputational: should the EU relax its standards of essential equivalence when member states' traveling residents are faced with its policies, the reputational damage to the standard exported through the Brussels effect would be great indeed (Bradford, 2020; Christakis, 2020).

7.2 Purpose limitation and function creep

The second problem is the undermining of purpose limitation-the doctrine that data collected for one purpose cannot be used for another purpose without authorization. The biography of Eurodac alone epitomizes the trend: introduced to allocate the asylum burden, it was broadened to serve law-enforcement databases in 2013 and transformed in 2024 into a "cross-purpose interoperability measure designed to serve security screening" (Regulation (EU) 2024/1358; Vavoula, 2022). Interoperability generalizes this drift, since a single hit to the

ESP retrieves results from databases that operate in distinct administrative realities (EDPS, 2018; Leese, 2022).

The trend becomes supranational with the use of external data pathways.

Finger data entered into the system from an asylum applicant's fingers to ascertain the handling Member State might soon be put to use to facilitate removal, provide to third state consulates, or-under an EBSP type scheme-enrich vetting databases belonging to states whose future governments, and future uses, are beyond the control of Europeans. Commentaries on the EU-US negotiating documents observed the inclusion of 'immigration offenses' amongst other 'risk criteria' to match on, and the capacity of the proposal to include compatible further processing to administrative procedures beyond the initial purpose for processing. While each individual usage can be justified in its own right, their collective path breaks down the intended partition from purpose.

7.3 Reciprocity asymmetry and coercive conditionality

The third challenge is one that is profoundly political. Sovereignty in the first instance is a right to say no, and conditionality seeks to undermine precisely that. This EBSP demand is not an offer for co-operation on terms of equal bargaining power.

It is a stick linked to a carrot-an unconditional right to visa-free travel that European publics take for granted.

This asymmetry is underscored by the fact that reciprocity on visa grants has been a long-term source of tension in EU-US relations, and various member states' citizens have long been excluded from the VWP. Although the EU has formally requested similar reciprocal data sharing with the US, and the VWP conditionality for immediate transfers already exists in the EES Regulation, reciprocity between actors with different types of capabilities is often superficial at best. The problem of the bilateral structure may be even more insidious. By treating the VWP as a bilateral construct, each Member State faces Washington individually, and any framework agreement will have to condone individual bilateral understandings, which translate a fundamental rights issue at EU level into 25 individual calculations of each member state's comfort level on travel convenience (Statewatch, 2025).

This is sovereignty that is not capable of much more than symbol, and this is precisely why the collective vs. Individual negotiation issue is itself a first-order sovereignty-political decision (Christakis, 2020; Floridi, 2020).

7.4 Accountability and remedies for data subjects

The fourth problem is the human flaw that lies behind all the treacherous templates. For their remedy to work under Article 47 of the Charter, a person must be able to know that her data was processed, be able to find who the accountable controller was, and be able to access an autonomous tribunal. Every external avenue bypasses one link of that chain.

Brouwer (2008) had documented the odds stacked against foreign citizens to remedy SIS alerts generated by other states; the challenge was magnified when the chain of processing traversed into a non-EEA legal space.

In return-related transfers, the data subject is necessarily being exported outside the legal space in which her remedies exist. In extraterritorial agency operations, the power balance over controllership is up for debate between Frontex, the host state, and Member State officials (Quintel, 2022). In Interpol-mediated screening, the punished record belongs to an institution beyond EU legal checks. And in the structure of the EBSP, the EDPB's query over whether an EU data subject could operationalize such rights under the US Privacy Act is still just a matter of speculation in the open literature (Statewatch, 2026).

There is an uncomfortably stark normative asymmetry within the very sovereignty discourse it condemns.

European concern over the EBSP has (uselessly) ensured that emphasis was laid on the biometric data of EU citizens alone. The Union's own databases hold the biometrics of a much higher number and a much broader scope of non-citizens, and the people who were at the greatest risk as a consequence of outward transfers – rejected asylum seekers and deportees – are the ones who attract the least political interest (Aas, 2011; FRA, 2018; Mitsilegas, 2015). A truly autonomous data

sovereignty can only be rights-based rather than forever just territorial, else it will only replicate at the international level the very double standard it has played such tiresome lip service to.

8. Discussion

The analysis leads to three conclusions. First, the issue of third-country access to EU biometric data does not just pose a "hypothetical danger," but is already a de facto reality transmitted via 5 pathways, each with a greatly varying degree of visibility. The overt EBSP has attracted scrutiny because of its abrupt and coercive nature, whereas the "silent" pathways of return cooperation, Interpol interfacing, and agency operations channel data or dependence abroad constantly and without public debate.

Second, "European data sovereignty" is most threatened from within: demand for external flows of data is driven by the EU's pursuit of faster returns and closer externalization, which the EDPS warns create an irrevocably changed environment; third parties largely exploit vacuums, or openings created by EU policy; sovereignty, in the three-dimensional sense established in Sec 3, is therefore being conceded gradually, not seized.

Third, the rights-based order does not appear passive, evidenced by Council's exclusion of central databases from the scope of the EBSP and interventions by the EDPS and EDPB, as well as the looming Schatten of Schrems II and Opinion 1/15: the relevant question is when, during the policy cycle, the power exercised by rights actually kicks in, or whether it merely acts as post-hoc correction after data infrastructure and expectations have become set, something which EDPS has warned us could be the point of no return.

Fairness must, admittedly, present the arguments to the contrary. Security cooperation with third countries clearly has practical benefits: facilitating the identification of dangerous travelers, disrupting fake documents, ensuring the returns without which any asylum system lacks any public legitimacy, the US argument about data sharing with Europe that they already do with European partners, and the rights of every state to control entries to its territory. Host governments are also within rights to say they cannot readmit their national citizens without determining their identity.

No argument is negligible, and "no" would likely be an untenable position in Europe; what is called for is not exclusivity but rigor, targeting not bulk, purpose defined not generic, independent not ad hoc control, real redress.

That is exactly the criterion the CJEU has now set out, and this is simply not a partisan approach, but applicable law in the context of the EU's legal order.

Multiple policy implications can be discerned. Firstly, external access must be negotiated on a Union-wide, not a bilateral, level (which the EBSP architecture facilitates, contrary to the ECJ stance), given that only a bloc negotiation can ensure meaningful "essential equivalence." All central databases must explicitly be exempted and access restricted to national, distributed, or derived databases, effectively filling the loophole discussed in Sec 6.5.

All third-country data subjects, regardless of their origin, should have the right to due process and independent supervision; data transfers must have clear time limits, prohibited re-transmission, and clauses of renewal with EDPS involvement.

With regard to the 'silent' channels, priority should be given to ensuring that Europol and Frontex provide transparency on data transfers abroad and, prior to further integration, work out an agreement with Interpol. Lastly, the double standard must be tackled head-on. The safeguards for citizens' personal data abroad which the EU requires for third countries' citizens in the EU are clearly measures of what the Union owes them.

9. Conclusion

This article aimed to describe the channels used by third countries to enter EU biometric migration databases and the implications that these channels have for the sovereignty over data for the EU. Methodologically, doctrinal and documentary analysis reveals five channels-data transfers related to returns, urgent law enforcement data transfers, the Interpol channel, agency-based agreements, and conditional arrangements-and that they each cumulatively challenge the adequacy benchmark, purpose limitation, reciprocity, and effective remedies. It argues that European

data sovereignty over migration biometrics is being eroded not so much by external invasion but by the internal logic of migration control and the reasons that it generates to permit the movement of identity data.

The EBSP negotiations consolidate all this into one dilemma: will the Union defend the standard of essential equivalence defined by its own Court-and face the real-world costs to the travel of its citizens-or will it sacrifice its citizens' biometric information for continued travel privileges?

Its contributions are to bridge two otherwise estranged literatures-fundamental rights challenges to EU migration databases and digital sovereignty-and to formulate a 3-dimensional conception of data sovereignty anchored in fundamental rights against which third country data arrangements can be appraised. Limits-the lack of interview data and classified agreements-outline the research agenda: empirical analysis of actual EBSP-type arrangements; comparison with other US requests to the UK, Australia, and Japan; and, most importantly, analysis of the subjective experience of data subjects, their travel, applications, or deportations, which forms the currency of such data transfers. If data sovereignty has any meaning at all under European law, its ability to protect data subjects must be taken into account.

References

Aas, K. F. (2011). 'Crimmigrant' bodies and bona fide travelers: Surveillance, citizenship and global governance. Theoretical Criminology, 15(3), 331–346. https://doi.org/10.1177/1362480610396643

Amoore, L. (2006). Biometric borders: Governing mobilities in the war on terror. Political Geography, 25(3), 336–351. https://doi.org/10.1016/j.polgeo.2006.02.001

Bellanova, R., & de Goede, M. (2022). The algorithmic regulation of security: An infrastructural perspective. Regulation & Governance, 16(1), 102–118. https://doi.org/10.1111/rego.12338

Bigo, D. (2014). The (in)securitization practices of the three universes of EU border control: Military/Navy, border guards/police, database analysts. Security Dialogue, 45(3), 209–225. https://doi.org/10.1177/0967010614530459

Boehm, F. (2012). Information sharing and data protection in the Area of Freedom, Security and Justice. Springer.

Bradford, A. (2020). The Brussels effect: How the European Union rules the world. Oxford University Press.

Broeders, D. (2007). The new digital borders of Europe: EU databases and the surveillance of irregular migrants. International Sociology, 22(1), 71–92. https://doi.org/10.1177/0268580907070126

Brouwer, E. (2008). Digital borders and real rights: Effective remedies for third-country nationals in the Schengen Information System. Martinus Nijhoff.

Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II), ECLI:EU:C:2020:559 (CJEU, 16 July 2020).

Case C-817/19, Ligue des droits humains v Conseil des ministres, ECLI:EU:C:2022:491 (CJEU, 21 June 2022).

Christakis, T. (2020). 'European digital sovereignty': Successfully navigating between the 'Brussels effect' and Europe's quest for strategic autonomy. Multidisciplinary Institute on Artificial Intelligence, Université Grenoble Alpes. https://doi.org/10.2139/ssrn.3748098

Council of the European Union. (2023). US Enhanced Border Security Partnership (Council doc. 8307/23). Brussels.

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? New Media & Society, 21(10), 2305–2322. https://doi.org/10.1177/1461444819865984

Dijstelbloem, H. (2021). Borders as infrastructure: The technopolitics of border control. MIT Press.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences (Law Enforcement Directive). OJ L 119, 4.5.2016, 89–131.

European Commission. (2021). Recommendation for a Council Decision authorising the opening of negotiations for a cooperation agreement between the European Union and the International Criminal Police Organisation (Interpol) (COM(2021) 177 final). Brussels.

European Commission. (2025). Recommendation for a Council Decision authorising the opening of negotiations on a framework agreement between the European Union and the United States of America on the exchange of information for security screenings and identity verifications relating to border procedures and applications for visa (COM(2025) 447 final). Brussels.

European Data Protection Supervisor. (2018). Opinion 4/2018 on the proposals for two regulations establishing a framework for interoperability between EU large-scale information systems. Brussels: EDPS.

European Union Agency for Fundamental Rights. (2018). Under watchful eyes: Biometrics, EU IT systems and fundamental rights. Publications Office of the European Union.

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. Philosophy & Technology, 33(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6

Glouftsios, G. (2021). Engineering digitised borders: Designing and managing the Visa Information System. Palgrave Macmillan.

Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications and Others, ECLI:EU:C:2014:238 (CJEU, 8 April 2014).

Leese, M. (2022). Fixing state vision: Interoperability, biometrics, and identity management in the EU. Geopolitics, 27(1), 113–133. https://doi.org/10.1080/14650045.2020.1830764

Mitsilegas, V. (2015). The criminalisation of migration in Europe: Challenges for human rights and the rule of law. Springer.

Opinion 1/15 of the Court (Grand Chamber) on the draft EU–Canada PNR Agreement, ECLI:EU:C:2017:592 (CJEU, 26 July 2017).

Quintel, T. (2022). Data protection, migration and border control: The GDPR, the Law Enforcement Directive and EU databases. Hart Publishing.

Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation). OJ L 218, 13.8.2008, 60–81.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). OJ L 119, 4.5.2016, 1–88.

Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES). OJ L 327, 9.12.2017, 20–82.

Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS). OJ L 236, 19.9.2018, 1–71.

Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks. OJ L 312, 7.12.2018, 14–55.

Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN). OJ L 135, 22.5.2019, 1–26.

Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa. OJ L 135, 22.5.2019, 27–84.

Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration. OJ L 135, 22.5.2019, 85–135.

Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard. OJ L 295, 14.11.2019, 1–131.

Regulation (EU) 2024/1358 of the European Parliament and of the Council of 14 May 2024 on the establishment of 'Eurodac' for the comparison of biometric data. OJ L, 2024/1358, 22.5.2024.

Statewatch. (2025, December 18). US access to EU citizens' biometric data: Ministers approve EU negotiating mandate. https://www.statewatch.org/news/2025/december/us-access-to-eu-citizens-biometric-data-ministers-approve-eu-negotiating-mandate/

Statewatch. (2026, May). EU–US data exchange proposal in conflict with EU laws. https://www.statewatch.org/analyses/2026/eu-us-data-exchange-proposal-in-conflict-with-eu-laws/

Trauttmansdorff, P., & Felt, U. (2023). Between infrastructural experimentation and collective imagination: The digital transformation of the EU border regime. Science, Technology, & Human Values, 48(3), 635–662. https://doi.org/10.1177/01622439211057523

Tzanou, M. (2017). The fundamental right to data protection: Normative value in the context of counter-terrorism surveillance. Hart Publishing.

Vavoula, N. (2022). Immigration and privacy in the law of the European Union: The case of information systems. Brill Nijhoff.