**The 'Puzzle' of EU Large-Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Personal Data Protection**

Niovi Vavoula*

**Abstract:** The past three decades have been marked by the proliferation of EU databases processing various personal data collected by different categories of third-country nationals. At present, three databases are fully operational; the second generation Schengen Information System (SIS II), the Visa Information System (VIS) and Eurodac. However, in the future three new databases will be set up; an Entry/Exit System (EES), a European Travel and Information Authorisation System (ETIAS) and a European Criminal Record Information System for third-country nationals (ECRIS-TCN). In addition, interoperability among these systems is in the making. By mapping the historical evolution of databases for third-country nationals in three distinct waves, this article demonstrates the progressive generalisation of their surveillance via the mass collection of their personal data, which are used in a multiplicity of purposes. Then, drawing on the jurisprudence of the European Courts, this article examines key privacy and data protection concerns concerning: the necessity of setting up or maintaining information systems, their personal scope, the categories of personal data processed, access to stored data for law enforcement purposes and interoperability among the systems.

## Introduction

The creation of EU large-scale information systems processing various personal data of different categories of third-country nationals is inextricably linked with the emergence of 'a Europe without internal frontiers'. The story begins in the mid-1980s with the addition of borders to the list of responsibilities shared by the Member States and the EU (then European Community). In parallel, a more limited number of Member States decided to abolish their internal border controls within the framework of the Schengen cooperation.[1] The dismantlement of internal checks was accompanied by so-called compensatory or flanking measures providing for, among other things, a common set of rules on external borders, short-stay visas and asylum applications. With the Treaty of Amsterdam, the so-called Schengen

* Lecturer in Migration and Security at Queen Mary University of London.

[1] The Schengen Agreement [2000] OJ L239/12; The Convention Implementing the Schengen Agreement (CISA) [2000] OJ L239/19.

*acquis*, was integrated within EU law.[2] At the same time, the EU competence in Justice and Home Affairs (JHA) was modified to achieve the establishment of an Area of Freedom, Security and Justice (AFSJ). Since then, efforts to control the movement of third-country nationals within the Schengen area have been coupled with efforts to prevent them from reaching the EU external border,[3] thus necessitating action outside the physical border.[4] In all of these developments, the growing tendency to associate third-country nationals with irregular migration and criminality has been critical. Asylum and visa applications, as well as entry and exit procedures, have been instrumentalised for the purpose of the prevention and investigation of crimes, particularly of terrorism.[5] More broadly speaking, security considerations have had a major impact in determining the objectives and rules of immigration control instruments.[6]

The evolution of digital technologies has been an indispensable component of these efforts. As Bonditti points out, technology has been the "servant mistress of politics"[7] resulting in "the digitalisation of the European migration policy".[8] In this framework, technological advances, particularly the most controversial ones, such as fingerprinting, "terrorist profiling" and travel surveillance, "have been (and are still being) 'tested' on migrants and refugees or otherwise legitimised at the border".[9] Biometry in particular has

[2] Council Decision 1999/435/ EC concerning the definition of the Schengen acquis for the purpose of determining, in conformity with the relevant provisions of the Treaty establishing the European Community and the Treaty on European Union, the legal basis for each of the provisions or decisions which constitute the acquis [1999] OJ L176/1.

[3] D. Bigo and E. Guild (eds), *Controlling Frontiers: Free Movement into and within Europe* (Aldershot: Ashgate, 2005); V. Mitsilegas, "Human Rights, Terrorism and the Quest for 'Border Security'" in M. Pedrazzi et al. (eds), *Individual Guarantees in the European Judicial Area in Criminal Matters* (Brussels: Bruylant, 2011), p.85; V. Mitsilegas, "Immigration Control in an Era of Globalisation: Deflecting Foreigners, Weakening Citizens, Strengthening the State" (2012) 19(1) *Indiana Journal of Global Legal Studies* 1, 3; V. Mitsilegas, "The Law of the Border and the Borders of Law: Rethinking Border Control from the Perspective of the Individual" in L. Weber (ed), *Rethinking Border Control for a Globalizing World* (Abingdon: Routledge, 2015), p.15.

[4] For an analysis see B. Ryan and V. Mitsilegas (eds), *Extraterritorial Immigration Control* (Leiden/Boston: Martinus Nijhoff, 2010).

[5] For instance, the Hague Programme states: "the management of migration flows, including the fight against illegal immigration, should be strengthened by establishing a continuum of security measures that effectively links visa application procedures and entry and exit procedures at external border crossings. Such measures are also of importance for the prevention and control of crime, in particular terrorism". The Hague Programme [2004] OJ C53/1, p.7.

[6] For instance, see Commission, "The European Agenda on Security" COM(2015) 185 final.

[7] P. Bonditti, "From Territorial Spaces to Networks: A Foucaultian Approach to the Implementation of Biometry" (2004) 29(4) *Alternatives: Global, Local, Political* 465.

[8] M. Besters and F. Brom, "'Greedy' Information Technology: The Digitalization of the European Migration Policy" (2010) 12(4) *European Journal of Migration and Law* 455.

[9] B. Hayes, "NeoConOpticon: The EU Security-Industrial Complex" (Transnational Institute/Statewatch, 2009), p.35; see K. Lindskov Jacobsen, "Making Design Safe for Citizens: A Hidden History of Humanitarian Experimentation" (2010) 14(1) *Citizenship Studies* 89.

been championed as a tool to reliably determine whether a third-country national is whom he claims to be.[10] The move to identify individuals based on their biological characteristics is attributed to a number of advantages of biometric over alphanumeric identifiers, including their universality, distinctiveness and permanence.[11]

Technological evolution has enabled the setting up of a "mille-feuille" of databases, currently comprising the Schengen Information System (SIS II, formerly named SIS), Eurodac; and the Visa Information System (VIS). The momentum for EU immigration databases is greater than ever. In addition to enhancements to the three existing databases, centralised systems are bound to proliferate via the establishment of an Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS) and the European Criminal Record Information System for third-country nationals (ECRIS-TCN). The different systems are established as separate entities, but in view of this compartmentalisation, interoperability – different ways of linking information from the different data pots – is also in the making. This elaborate framework exemplifies the gradual transformation of traditional immigration control to a system of surveillance, whereby different groups of third-country nationals are classified according to the dangers they pose to society and surveillance techniques become the vehicle for managing these dangers.[12] As Gammeltoft-Hansen has observed, EU databases operate as a series of concentric "risk filters" serving to categorise and identify migrants.[13] Broeders has framed databases as forming part of "panopticon Europe", an ever-growing strategy designed to exclude third-country nationals through delegitimatisation and criminalisation.[14] Bigo has instead coined the term "banopticon", designed to highlight the fact that these systems are not intended to monitor everybody, but

[10] For a thorough analysis on biometrics see E. Kindt, *Privacy and Data Protection Issues of Biometric Identifiers* (Dordrecht: Springer, 2013).

[11] A. Jain, R. Bolle, and S. Pankanti, *Biometrics. Personal Identification in Networked Society* (Dordrecht: Springer, 2006). For an analysis of implementing biometrics at the borders see Commission, "Biometrics at the Frontiers: Assessing the Impact on Society" (2005). Their reliability has been criticised by E. Guild, S. Carrera and A. Eggenschwiler, "Informing the Borders Debate" (CEPS, 2009), p.3.

[12] A. Baldaccini, "Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases" (2008) 10(1) E*uropean Journal of Migration and Law* 31; V. Mitsilegas, "Border Security in the European Union: Towards Centralised Controls and Maximum Surveillance" in E. Guild et al. (eds), *Whose Freedom, Security and Justice? EU Immigration and Asylum Law and Policy* (Oxford: Hart, 2007), p.359; V. Mitsilegas, "The Border Paradox: The Surveillance of Movement in a Union without Internal Frontiers" in H. Lindahl (ed), *A Right to Inclusion and Exclusion? Normative Fault Lines of the EU's Area of Freedom, Security and Justice* (Oxford: Hart, 2009), p.33.

[13] T. Gammeltoft-Hansen, "Filtering Out the Risk Migrant: Migration Control, Risk Theory and the EU" (Working Paper 52/2006, AMID Working Paper Series, 2006), p.8.

[14] D. Broeders, "The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants" (2007) 22(1) *International Sociology* 71.

only the designated risk groups, constituting an exclusionary form of control that seeks to banish and prevent or deny entry.[15]

Against this background, this article maps the complex landscape of EU centralised databases involving third-country nationals by tracing three historical periods in the surveillance of movement: the initial steps to employ technological means for purposes of immigration control and law enforcement; the systematisation of immigration databases and the gradual expansion of their capacities; and the current stage of generalised and normalised surveillance through the processing of personal data of practically the entire foreign population. This article offers an anthology of privacy and data protection challenges, based on the jurisprudence of the Court of Justice of the EU (CJEU) and the European Court of Human Rights (ECtHR). The assessment focuses on the necessity of setting up or maintaining information systems, their personal scope, the categories of personal data processed, access to stored data for law enforcement purposes and interoperability among the systems.

## Surveillance of Third-Country Nationals in Three Waves

### *The First Wave: Establishing Centralised Databases to Modernise Immigration Control*

In the early 1990s, the first EU immigration databases were created: the SIS and Eurodac. At the time, the technology was still fairly rudimentary, and therefore these two databases necessarily followed a compartmentalised approach.

#### Keeping Away the Unwanted: The SIS

At the heart of the compensatory measures for the abolition of internal border controls,[16] the SIS became operational in 1995.[17] The system holds alerts on various categories of persons and objects, in particular on persons wanted for arrest and extradition,[18] missing persons,[19] witnesses or persons summoned to appear before the judicial authorities or to serve a penalty,[20] persons or objects subject to discreet surveillance (where the individual is not made

[15] D. Bigo, "Globalized (In)Security: The Field and the Ban-Opticon" in D. Bigo and A. Tsoukala (eds), *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11* (Dordrecht: Routledge, 2008).

[16] B. Schattenberg, "SIS: Privacy and Legal Protection" in H. Schermers et al. (eds), *Free Movement of Persons in Europe: Legal Problems and Experience* (Leiden/Boston: Martinus Nijhoff, 1993), p.43.

[17] For a detailed overview of the SIS see E. Brouwer, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System* (Leiden/Boston: Martinus Nijhoff, 2008), pp.47–57.

[18] Art.95 CISA.

[19] Art.97 CISA.

[20] Art.98 CISA.

aware of the surveillance) or specific checks[21] and objects sought for the purpose of seizure or their use as evidence in criminal proceedings.[22] In addition, the SIS stores alerts on third-country nationals to be refused entry or stay in the Schengen area.[23] The variety of possible alerts reflect the system's overall purpose of ensuring a high level of security in the Schengen area by facilitating both border control and police investigations.[24] In practice, alerts on third-country nationals dominate the system.[25] Data may be inserted on two main grounds;[26] First, when the third-country national poses a threat to public policy, public security or national security. This could be the case either when they had been convicted of an offence carrying a custodial sentence of at least one year,[27] or there were serious grounds for believing that they had committed serious criminal offences, or there was clear evidence that they planned to commit such offences.[28] The second ground for inserting alerts involves irregular migrants subjected to deportation, refusal of entry or removal, including or accompanied by a prohibition on entry or, where applicable, a prohibition on residence.[29] In both cases, registration was not mandatory and depended upon a national administrative or court decision.[30] In connection with each alert, the SIS initially stored basic alphanumeric information – name, nationality, the type of alert, any specific objective physical characteristics– and operated on a hit/no hit basis. In the event of a hit, national authorities would perform searches for supplementary information in another system named Supplementary Information Request at the National Entries (SIRENE).

The 'Truth Serum': Eurodac

Parallel to the establishment of the SIS, national governments set out common rules –the Dublin rules- on how to determine which Member State would be responsible for examining asylum applications based on prescribed hierarchical criteria.[31] A necessary corollary was a

[21] Art.99 CISA.
[22] Art.100 CISA.
[23] Art.96 CISA.
[24] Art.93 CISA.
[25] E. Guild, "Moving the Borders of Europe" (Inaugural lecture, University of Nijmegen, 2000), p.24; Brouwer, *Digital Borders and Real Rights,* pp.66–68; Schengen Joint Supervisory Authority, "Final Report of the Schengen Joint Supervisory Authority on the Follow-Up of the Recommendations Concerning the Use of Article 96 Alerts in the Schengen Information System" (2010).
[26] Under art.96, CISA all alerts were inserted at the discretion of national authorities, on the basis of a national decision either by an administrative or judicial authority.
[27] Art.96(2)(a) CISA.
[28] Art.96(2)(b) CISA.
[29] Art.96(3) CISA.
[30] Art.96(1) CISA.
[31] Dublin Convention determining the EU Member State responsible for examining an application for asylum lodged in one of the EU Member States [1997] OJ C254/1, replaced by Regulation 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining

central registry that would process the fingerprints of asylum seekers to assist in the implementation of Dublin. Eurodac was created by Regulation 2725/2000[32] (supplemented by Regulation 407/2002[33] and became operational in 2003.[34] According to its basic rules, Member States must take the fingerprints of every asylum seeker over the age of fourteen when they apply for international protection. The collected fingerprints are compared with fingerprints already transmitted by other participating countries.[35] If a Eurodac check reveals that the fingerprints have already been recorded in another Member State, the asylum seeker may be sent to that Member State, if no other Dublin criteria are applicable. In addition, the system processes the fingerprints of all migrants that are apprehended in connection with irregular border crossings.[36] As for the fingerprints of third-country nationals found irregularly staying on the territory of a Member State, these may be transmitted for comparison on the spot with the existing Eurodac and they are not centrally stored.[37] Both groups are also connected with the operation of the Dublin system, as a key criterion for assigning responsibility among the Member States is the asylum seeker's country of first entry into the EU.[38] As for the type of data stored in Eurodac, apart from a full set of fingerprints, it only contains limited biographical information.[39] However, the fingerprints of migrants found irregularly staying are not centrally stored, but only compared with existing records for the sole purpose of determining whether the irregular migrant has formerly applied for international protection in another Member State.

*The Second Wave: Immigration Databases and the "War on Terror"*

The events of 9/11 signaled a new era for EU databases marked by the intertwining between immigration and security. The migration-risk nexus -fuelled by the events in the US, and then the attacks in Madrid (2004) and London (2005)- coincided with technological advances, and

---

an asylum application lodged in one of the Member States by a third-country national [2003] OJ L50/1 (Dublin II Regulation) and Regulation 604/2013 [2013] OJ L180/31 (Dublin III Regulation). The Dublin IV Regulation is currently being negotiated. See Commission, COM(2016) 270 final.

[32] Regulation 2725/2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention [2000] OJ L316/1.

[33] Regulation 407/2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention [2002] OJ L62/1.

[34] For a detailed overview see J. Aus, "Eurodac: A Solution Looking for a Problem?" (2006) 10 *European Integration online Papers* 1.

[35] Arts4-7 of Regulation 2725/2000.

[36] Arts8–10 of Regulation 2725/2000.

[37] Art.11 of Regulation 2725/2000.

[38] Art.13 of Regulation 604/2013.

[39] For an analysis see E. Guild, "Unreadable Papers? The EU's First Experiences with Biometrics: Examining Eurodac and the EU's Borders" in J. Lodge (ed), *Are You Who You Say You Are? The EU and Biometric Borders* (Nijmegen: Wolf Legal Publishers, 2007), p.32.

the combination resulted in the creation of a new database (VIS) and the expansion of old ones.

Targeting Visa Applicants: The VIS

Visas became a matter of collective interest in the Schengen framework, which contained extensive rules on short-stay (Schengen) visas,[40] supplemented by provisions on freedom to travel.[41] With the entry into force of the Amsterdam Treaty, EU competences in the field of short-stay visas were significantly reinforced.[42] However, progress on establishing a common visa policy was rather slow until the events of 9/11, when the EU Member States decided to establishing a network for information exchange among their national authorities responsible for issuing short-stay visas.[43] The premise was that visa applicants constitute a risky population, justifying measures that would potentially pre-empt and deter their movement. As was explicitly stated:

> "(t)he events of 11 September 2001 … radically altered the situation, showing that visas are not just about controlling immigration but are above all an issue of EU member states' internal security".[44]

The VIS was set up by a series of instruments: Decision 2004/512/EC,[45] which formed the legal basis for the VIS; Regulation 767/2008[46] governing the use of the system for border control purposes; and Council Decision 2008/633/JHA[47] prescribing the modalities by which visa data was to be consulted by law enforcement authorities and Europol. The VIS is a multi-purpose tool: its overarching purpose is to improve the implementation of the common visa policy, but no fewer than seven sub-purposes are envisaged, including the fight against fraud and visa shopping and the contribution to the prevention of threats to Member States'

[40] Arts9-17 CISA. The duration of a short-stay is no more than three months in any six-month period from the date of first entry in the territory of the Member State.
[41] Arts19–24 CISA. Long-term visas remain regulated at national level only.
[42] Arts62(2)(b), 62(3), 67 TFEU. For an overview see A. Meloni, "The Development of a Common Visa Policy under the Treaty of Amsterdam" (2005) 42(5) *Common Market Law Review* 1357.
[43] For an overview of the discussions see Council Documents 12019/01 (20.09.2001); 14523/01 (26.11.2001); 15577/01 (21.122001); SN 300/1/01 (15.12.2001).
[44] Council Document 14523/01 (26.01.2002).
[45] Council Decision 2004/512/EC establishing the Visa Information System (VIS) [2004] OJ L213/5.
[46] Regulation (EC) 767/2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas [2008] OJ L218/60, as amended by Regulation (EC) 810/2009 [2009] OJ L243/1 (VIS Regulation).
[47] Council Decision 2008/633/JHA concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences [2008] OJ L218/129 (VIS Decision).

internal security.[48] The system stores a wide array of personal data of visa applicants, including biographic information, biometrics (a full set of fingerprints and a photograph), information on persons who have issued an invitation and/or are liable to pay for the applicant's subsistence costs, purpose of the travel, residence and occupation.[49] Access to VIS data for law enforcement purposes is not routinely granted, but only when necessary in a specific case, and only when there are reasonable grounds to believe that consultation of the system will substantially contribute to the prevention, detection or investigation of terrorist offences and other serious crimes.[50] These conditions must be verified by the Member State's Central Access Point following a request by a designated authority.[51] More ambiguously, access to VIS data by Europol is allowed "within the limits of its mandate and when necessary for the performance of its tasks".[52]

The Transformation of the SIS into an Investigation Tool

A second strand of action has been the reinforcement of the functions of the SIS. At a Spanish initiative, Regulation 871/2004[53] and Council Decision 2005/211/JHA[54] were adopted, stipulating wider access to certain types of data by visa, judicial and law enforcement authorities, including Europol and Eurojust. In the case of Europol, however, access was not granted to immigration data. Furthermore, the pressing need to develop a second generation SIS – the SIS II – so as to accommodate the expanded EU family after the 2004 enlargement was seen as a first-class opportunity to insert new functionalities into the system.[55] Consequently, two Regulations and a Decision were formally adopted in 2006;[56] however,

[48] For a critical examination of the VIS purposes see N. Vavoula, *Immigration and Privacy in the Law of the European Union: The Case of Databases* (Leiden/Boston: Brill Nijhoff, forthcoming 2020), Ch.3. The ranking of the purposes has been litigated before the EU Court of Justice. See *UK v. Council* (C-482/08) ECLI:EU:C:2010:631.

[49] Art.9 of Regulation 767/2008.

[50] Art.5(1) of Decision 2008/633/JHA.

[51] Art.4 of Decision 2008/633/JHA.

[52] Art.7 of Decision 2008/633/JHA.

[53] Regulation 871/2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism [2004] OJ L162/29.

[54] Council Decision 2005/211/JHA concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism [2005] OJ L68/44.

[55] For an overview see J. Parkin, "The Difficult Road to the Schengen Information System II - The Legacy of Laboratories and the Cost for Fundamental Rights and the Rule of Law" (CEPS, 2011).

[56] Regulation 1987/2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2006] OJ L381/4 (SIS II Regulation); Council Decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2007] OJ L205/63 (SIS II Decision); Regulation 1986/2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates [2006] OJ L381/1.

due to numerous technical complications the SIS II only commenced its operation in April 2013.

The reforms made to the SIS II mark its gradual transformation from a mere reporting mechanism to a general investigation tool.[57] One major shift has been the possibility of interlinking alerts involving different individuals or events that are inserted under different legal bases.[58] Such interlinking is allowed only if there is a clear operational need. The potential for profiling through the interlinking of alerts is significant: "the person is no longer 'assessed' on the basis of data relating only to him/her, but on the basis of his/her possible association with other persons".[59] Even though authorities with no right of access to certain categories of alert will not be able to see the link to an alert to which they do not have access, such authorities will not necessarily be unaware of the existence of a link.[60]

Another major change involves the possibility of including biometric identifiers (photographs and fingerprints) within the system.[61] This change is part of a more general trend to introduce biometrics in all EU databases.[62] According to Article 22 of the SIS II Regulation, biometrics would be introduced in two phases: (i) in the first stage, they will be used only for identity verification (one-to-one searches); (ii) the second stage would allow the use of the biometrics to identify other individuals (one-to-many searches). This development has significant implications: it transforms the database into a general intelligence weapon, as biometrics can be used in the course of investigations to conduct speculative searches in the database's pool of suspected population, the so-called fishing expeditions.[63] A Commission report on the readiness and availability of fingerprints for identification purposes confirms these concerns, as it is stated that a comparison of fingerprints with those already stored "might identify links with other alerts".[64]

---

[57] It must be noted that under the revised SIS II rules, the registration of alerts on public policy, public security and national security grounds is mandatory. See art.24 of Regulation 1986/2006.

[58] For examples of interlinking see Council Document 12573/3/04 (30.11.2004), p.3.

[59] European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the establishment, operation and use of the Second Generation Schengen Information System", p.46.

[60] V. Mitsilegas, *EU Criminal Law* (Oxford: Hart, 2009), p.241.

[61] Art.22 of Regulation 1986/2006.

[62] E. Brouwer, "The Use of Biometrics in EU Databases and Identity Documents: Keeping Track of Foreigners' Movements and Rights" in J. Lodge (ed), *Are You Who You Say You Are? The EU and Biometric Borders* (Nijmegen: Wolf Legal Publishers, 2007), pp.45–66. See Baldaccini, "Counter-Terrorism and the EU Strategy for Border Security".

[63] B. Hayes, "From the Schengen Information System to the SIS II and the Visa Information System (VIS): The Proposals Explained" (Statewatch, 2004), p.4; Baldaccini, "Counter-Terrorism and the EU Strategy for Border Security", p.38.

[64] Commission, "The availability and readiness of technology to identify a person on the basis of fingerprints held in the second generation Schengen Information System (SIS II)" COM(2016) 93 final, p.7.

The Use of Eurodac Data for Law Enforcement Purposes

A paradigmatic example of how the boundaries between immigration and police databases have been blurred is the re-configuration of Eurodac to a tool in the fight against serious terrorism and serious crime. A year after the database had begun its operation, the Hague Programme called for the maximisation of effectiveness and interoperability of EU information systems and "an innovative approach to the cross-border exchange of law enforcement information".[65] Shortly afterwards, the Commission published a Communication on improved effectiveness, enhanced interoperability and synergies of EU information systems stating that

> "authorities responsible for internal security could … have access to Eurodac in well-defined cases, when there is a substantiated suspicion that the perpetrator of a serious crime had applied for asylum".[66]

After four proposals and largely under the pressure of finalising the second phase of the Common European Asylum System (CEAS),[67] the recast Eurodac Regulation was adopted in June 2013,[68] opening up the databases to law enforcement authorities and Europol.

As with the VIS, law enforcement access is listed as an ancillary purpose. Consultation of Eurodac data involves only the prevention, detection and investigation of terrorist offences and other serious crimes.[69] The conditions for access are stricter than the ones prescribed in the VIS Decision.[70] In particular, there is an additional step for accessing the Eurodac data: the national authority must have already consulted national fingerprint

[65] The Hague Programme, p.7.

[66] Commission, "Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs" COM(2005) 597 final.

[67] B. Juster and V. Tsianos, "Erase Them! Eurodac and Digital Deportability" (Transversal/EIPCP Multilingual Webjournal, February 2013) http://eipcp.net/transversal/0313/kuster-tsianos/en.

[68] Regulation 603/2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice [2013] OJ L180/1 (recast Eurodac Regulation).

[69] Recital 31.

[70] These conditions apply also in the case of Europol access to Eurodac data. For an evaluation see European Data Protection Supervisor, "on the amended proposal for a regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No […/…] (recast)" [2013] OJ C28/3, para.54; Standing Committee of Experts on International Immigration, Refugee and Criminal Law (Meijers Committee), Note on the Proposal for a Regulation on the Establishment of Eurodac (COM(2012)254) (CM1216, 2012).

databases, as well as the automated fingerprinting identification systems (AFIS) of other Member States[71] and the VIS, and such consultation must have proven futile.[72] Furthermore, the necessity of consulting the database is defined more carefully: according to Article 20(1)(b), "there must be an overriding public security concern which makes the searching of the database proportionate". Verification that these data access conditions have been met is entrusted to a verifying authority assigned at the national level.

*The Third Wave: The Generalisation of Surveillance of Movement of Third-Country Nationals*

The most recent burst of databases-related activity has been prompted by the terrorism events across EU Member States since 2015. A number of proposals that had remained in the EU legislative drawer for years re-emerged as part of a comprehensive response at EU level, encapsulated in the concept of establishing a "genuine Security Union".[73] Overall, the development of databases has accelerated tremendously: new systems have been established to fill perceived "informational gaps" created by the compartmentalised approach of the 1990s and 2000s; the existing systems have been refurbished to enhance and magnify their use; and interoperability among the systems has been heavily promoted.

Visa-Free Travellers as a Risk: The EES and the ETIAS

Though creating a rather comprehensive framework, the aforementioned databases do not cover those individuals originating from countries not subject to the visa regime. Therefore, influenced by similar initiatives in the US, in 2013 the Commission presented three legislative proposals commonly referred to as the "Smart Borders Package", including a proposal to establish an Entry/Exit System (EES).[74] Due to proportionality concerns,[75] the Commission originally left the registration of biometrics and law enforcement access outside the scope of that proposal, and later entirely withdrew the package. However, in the aftermath of the 2015

[71] Such consultation is conducted on the basis of Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime [2008] OJ L210/1 (Prüm Decision).

[72] Art.20(1) of Regulation 603/2013. There is a caveat: prior consultation is not necessary if there are reasonable grounds to believe that a comparison with such systems would not lead to the establishment of the identity of the data subject.

[73] See Commission, "The European Agenda on Security".

[74] Commission, "Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union" COM(2013) 95 final. The other proposals involved a "Registered Travellers Programme" (RTP) (COM(2013) 97 final) and amendments to the Schengen Borders Code (COM(2013) 96 final).

[75] For criticism, see among others Article 29 Data Protection Working Party, "Opinion 05/2013 on Smart Borders" (WP206, 2013); Standing Committee of Experts on International Immigration, Refugee and Criminal Law (Meijers Committee), "Note on the Smart Borders proposals (COM(2013) 95 final, COM(2013) 96 final and COM(2013) 97 final)" (CM1307, 2013).

terrorist events, the EES returned in the EU agenda, including a far-reaching suggestion to further extend the reach of the EES to cover EU nationals.[76] Though this proposal has been (so far) set aside due to difficulties in finding a legal basis without jeopardising free movement rights,[77] it indicates the undertone of a highly securitised framework in the post-2015 era.[78] A revised EES proposal was released in April 2016,[79] and the EES was ultimately adopted in November 2017.[80] Though certain rules were slightly modified, the basic policy choices remained the same.

The system will register border crossing both at entry and exit for all third-country nationals admitted for a short stay, irrespective of whether they are required to obtain a Schengen visa or not.[81] It will also apply to third-country nationals whose entry for a short stay has been refused at the border, which means that even though these persons will be physically kept outside of the EU, their data will be stored in the EES for future use. Following the VIS model, the EES is a multi-purpose tool: it will enhance the efficiency and automation of border checks; assist in the identification of irregular migrants and overstayers; combat identity fraud and misuse of travel documents; and strengthen internal security and the fight against terrorism by allowing law enforcement authorities access to travel history records.[82] To these ends, it will record the identities of third-country nationals, by storing alphanumeric data, four fingerprints and a facial image, along with details of their travel documents, which will be linked to electronic entry and exit records.[83] The retention periods foreseen vary depending on whether an exit record exists or not; if so, it is three years, but in

[76] Council Document 12272/15 (25.09.2015).
[77] Council, Document 13193/15 (17.11.2015), p.8.
[78] The EDPS refers to a letter written to the European Council of October 2015, where it is stated that "such technical solutions could also be explored for EU citizens, to address security challenges". See Giovanni Buttarelli, "A data protection perspective on the Smart Border Package – focusing on the possibility of law enforcement authorities' access to border data" (2015) 3. To my knowledge no subsequent documentation touches upon this aspect.
[79] Commission, "Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011" COM(2016) 194 final.
[80] Regulation 2017/2226 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 [2017] OJ L32720 (EES Regulation).
[81] According to art.2(3), there are a few exceptions: those who have residence permits; are family members of an EU national and hold a residence card; or are family members of another third-country national who enjoys free movement rights or has a residence card.
[82] Art.6(1).
[83] Arts14–20.

case of potential overstayers, the records will be kept for five years.[84] The current practice of stamping travel documents will be abolished and an information mechanism will be included to identify cases where there are no records of exit.[85] Access to EES data for the purposes of the prevention, detection and investigation of terrorist offences and other serious crimes is envisaged under a mixture of rules combining the Eurodac and the VIS models.[86] For example, verification that the conditions of access have been met is the responsibility of each Member State's Central Access Point.[87] Furthermore, the EES Regulation allows national authorities to search the database to identify "an unknown suspect perpetrator or suspected victim of a terrorist offence or other serious criminal offence" if they meet the listed conditions and have already (unsuccessfully) consulted their national databases or, in the case of fingerprints, their national AFIS.[88]

The movement of visa-free travellers will also be monitored through the European Travel Information and Authorisation System (ETIAS), enacted in September 2018.[89] The ETIAS was initially conceptualised alongside the EES,[90] but in 2011, the project was shelved

> "as the potential contribution to enhancing the security of the Member States would neither justify the collection of personal data at such a scale nor the financial cost and the impact on international relations".[91]

Following the removal of numerous countries from the 'black' list of countries whose nationals require a visa to enter the Schengen territory and under the influence of terrorist events, the idea re-emerged.[92] The ETIAS Regulation solidifies the link between immigration control and security, as one of its main objectives is to contribute to a high level of security by thoroughly assessing whether travellers pose a "security risk".[93] There are many other purposes of the database: preventing illegal migration, protecting public health, enhancing the effectiveness of border checks, supporting the SIS II, and contributing to the prevention, detection and investigation of terrorist offences or of other serious criminal offences.[94] To

[84] Art.34.
[85] Art.12.
[86] Arts29–33.
[87] Art29. Compare with art.3 of the VIS Decision.
[88] Art.32(2). Compare with art. 20(1) of the recast Eurodac Regulation.
[89] Regulation 2018/1240 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 [2018] OJ L61/1 (ETIAS Regulation).
[90] Commission, "Preparing the next steps in border management in the European Union" COM(2008) 69 final.
[91] Commission, "Smart borders - options and the way ahead" COM(2011) 680 final, p.7.
[92] Commission, "Stronger and Smarter Information Systems for Borders and Security" COM(2016) 205 final, p.13.
[93] Art.4(a.
[94] Art.4(b)–(f).

achieve these aims, all visa-exempt travellers shall be obliged to obtain authorisation prior to their departure through an online application in which they must disclose a series of personal data including biographical data, travel arrangements, home and email address, phone number, level of education and current occupation.[95] The pre-screening and provision of authorisation shall take place on the basis of cross-checking against: (a) data held in existing immigration and law enforcement databases; (b) screening rules enabling profiling on the basis of risk indicators;[96] and (c) a special ETIAS watch list of individuals suspected of having participated in terrorism or other serious crimes or in respect of whom there are factual indications or reasonable grounds to believe that they will commit such offences.[97] If authorisation is granted, data will be held for three years; otherwise, it will be held for five years.[98] Law enforcement authorities and Europol will be granted access under rules largely mirroring those in the EES Regulation.[99]

Coupled with the EES, the ETIAS will constitute both a massive catalogue of third-country nationals and a powerful surveillance tool driven by the logic of risk prevention transplanted once again into immigration control.[100] However, a key distinction between the two systems lies in their scope and function; whereas the EES will monitor the entries and exits of almost all third-country nationals, the ETIAS imposes pre-screening requirements specifically to visa-free travellers. This is where the novelty of the ETIAS lies; an EES may detect and prevent the entry of unwelcomed third-country nationals at the moment of the border crossing only, whereas the ETIAS is a tool of extraterritorial control, closer to the operation of the VIS and an ETIAS authorisation is a light form of a visa requirement, which is oriented towards preventing the movement of potentially risky visa-free nationals already at the country of origin. In doing so, the ETIAS is understood as a platform for mining and profiling personal data, not simply issuing automated or manual travel authorisation decisions. The ETIAS screening rules are meant to identify persons who are otherwise unknown to national competent authorities but are assumed to be of interest for immigration control or security purposes and therefore are likely to commit criminal offences in the future. These persons will be flagged because of any specific actions they have engaged in but

[95] Art.17.
[96] Art.33.
[97] Art.34.
[98] Art.5.
[99] Arts50–53.
[100] Vavoula, *Immigration and Privacy in the Law of the EU*, Ch.6.

because they display particular category traits in a probabilistic logic devoid of concrete evidence.[101]

The SIS II, Eurodac and VIS under Refurbishment

Efforts to fill in "informational gaps" have been accompanied by radical reforms to all three operational databases. The Eurodac proposal,[102] tabled since May 2016, signals a landmark change in Eurodac's purpose – from a system aimed at the effective implementation of the Dublin mechanism into an instrument for wider immigration purposes, including the return of irregular migrants. The anticipated Eurodac reform is both quantitative and qualitative. Quantitavely, the personal scope has been expanded and additional categories of data are to be entered into the system, such as a facial image.[103] The age threshold for fingerprinting children is significantly reduced to the age of six.[104] The categories of data held in the database are also considerably expanded, in order to "allow immigration and asylum authorities to easily identify an individual".[105] Furthermore, information on persons who are found irregularly present on the national territory will be centrally stored. As these new categories of persons and information suggest, the transformation is also qualitative: Eurodac has been detached from its original Dublin context and re-conceptualised as a multi-purpose immigration tool.

The SIS II was also re-jigged.[106] Following an evaluation of the system, which found that a major flaw was the lack of harmonised national criteria for entering alerts,[107] the new

[101] S. Alegre, J. Jeandesboz, and N.Vavoula, "European Travel Information and Authorisation System (ETIAS): Border Management, Fundamental Rights and Data Protection" (Study for the European Parliament, PE 583.148, 2017), pp.23–26.

[102] Commission, "Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] , for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast)" COM(2016) 272 final. Agreement has been reached, but due to complications in relation to other asylum-related files, formal adoption is still pending.

[103] Art.2(1).

[104] Art.2(2).

[105] Art.13.

[106] Regulation 2018/1860 on the use of the Schengen Information System for the return of illegally staying third-country nationals [2018] OJ L312/1; Regulation 2018/1861 n the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 [2018] OJ L312/14.

[107] Commission, "Report from the Commission to the European Parliament and the Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with art. 24

legal bases rectify this issue, albeit taking the lowest-common-denominator approach and making the registration of entry bans and return decisions mandatory irrespective of an individual assessment.[108]

As for the VIS reform, it seeks to fill the one outstanding gap in the coverage of third-country nationals in EU databases – holders of residence permits, residence cards and long-stay visa holders.[109] The VIS proposal[110] extends the system to these groups of third-country nationals as well as lower the threshold age for fingerprinting (six years). With this reform, almost all third-country nationals will be monitored. The only exception will be family members of EU nationals who hold residence cards and thus benefit from free movement rights. The underlying logic for including legal residents and long-stay holders is the need to manage a decentralised system of residence permits issued at the national level, but this decentralised structure has been deemed to have a collateral effect on immigration control and security.[111] In particular, the inability to verify biometrically the identities of residence card and long-stay visa holders is considered a security risk.

The ECRIS-TCN: Bridging Law Enforcement with Immigration Control and Non-EU with EU Nationals?

The latest member in the databases' family is the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN).[112] The latter emerged as a necessity in the law enforcement context, as in order to obtain complete information on previous convictions of third-country nationals, requesting Member States were obliged to send 'blanket requests' to all Member States, thus creating a heavy administrative burden. The ECRIS-TCN will be a centralised system for the exchange of criminal records on convicted third-country nationals and stateless persons and is meant to complement the already existing,

(5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and art. 59 (3) and 66 (5) of Decision 2007/533/JHA" COM(2016) 880 final.

[108] Art.3 of Regulation 2018/1860; Art.24 of Regulation 2018/1861.

[109] For the discussion on the merits of registering residence permit holders see Council Document 12527/15 (8.10.2015).

[110] Commission, "Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA" COM(2018) 302 final.

[111] Art.1(2).

[112] Regulation 2019/816 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 [2019] OJ L135/1 (ECRIS-TCN Regulation); Directive 2019/884 amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA [2019] OJ L151/143.

decentralised ECRIS system through which information on the criminal records of EU nationals is exchanged among Member States. In cases where a record exists, data will be transferred by the convicting Member State to the requesting Member State on a bilateral basis. All queries will be submitted through the central ECRIS-TCN system, which will contain biographical and biometric data; the retention period is not universal and will depend upon the retention period for the criminal records in the national databases. A particularly thorny issue involves the inclusion of dual nationals -EU citizens who also hold the nationality of a third State- which creates potential discrimination compared to other EU citizens.[113]

Compartmentalisation Is Dead! Long Live Interoperability

With almost all third-country nationals effectively captured by at least one database, the final step towards an EU "Big Brother" is the interconnection of the different 'data pots' under the umbrella term of interoperability. In its 2005 Communication, the Commission defined interoperability as the "ability of IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge".[114] However, details on the legal aspect of interoperability were spared, as the concept was reduced to a technical rather than a legal or political matter.[115] Since the Paris attacks of 13 November 2015, the connection of the "data jars" has gained fresh impetus,[116] leading to the release of two proposals[117] that were officially adopted in May 2019.[118]

[113] See Council Document 10828/18 (10.07.2018).

[114] See Commission, COM(2005) 597 final.

[115] For a critique see P. De Hert and S. Gutwirth, "Interoperability of Police Databases within the EU: An Accountable Political Choice?" (2006) 20(1-2) *International Review of Law Computers & Technology* 21–22; European Data Protection Supervisor, "Comments on the Communication of the Commission on interoperability of European databases" (10.032006).

[116] European Council, EUCO 28/15 (18.12.2015), p.3; Council Document 7371/16 (24.03.2016), pt.55. A High Level Expert Group on Information Systems and Interoperability was appointed and it delivered its final report in May 2017. See High Level Expert Group on Information Systems and Interoperability, Final Report (May 2017).

[117] Commission, "Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)" COM(2017) 794 final; "Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226" COM(2017) 793 final. The proposals were replaced in June 2018. See Commission, "Amended proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) and amending [Regulation (EU) 2018/XX [the Eurodac Regulation],] Regulation (EU) 2018/XX [the Regulation on SIS in the field of law enforcement], Regulation (EU) 2018/XX [the ECRIS-TCN Regulation] and Regulation (EU) 2018/XX [the eu-LISA Regulation" COM(2018) 480 final; "Amended proposal for a Regulation of the European Parliament and of the

Interoperability is conceived as information systems "speaking to each other" and as an evolutionary tool that will enable further uses through the aggregation of data from different sources. Its four main components are a European Search Portal (ESP), a shared Biometric Matching Service (BMS), a Common Identity Repository (CIR) and a Multiple Identity Detector (MID). The ESP will enable competent authorities to simultaneous query the underlying systems and the combined results will be displayed on one single screen. Even though the screen will indicate in which databases the information is held, access rights will remain unaltered.[119] The BMS will generate and store templates from all biometric data recorded in the underlying systems, thus effectively becoming a new database that compiles biometrics from the SIS II, VIS, Eurodac, EES and ECRIS-TCN. At the core of interoperability lies the CIR, which will store an individual file for each person registered in the systems, containing both biometric and biographical data as well as a reference indicating the system from which the data were retrieved.[120] CIR's main objectives are to facilitate identity checks of third-country nationals, assist in the detection of individuals with multiple identities and streamline law enforcement access.[121] With respect to law enforcement, the rules explained earlier are substituted by a two-step process in which law enforcement authorities can first consult all databases to check whether records on an individual exist in any of the databases without obtaining prior authorisation by a verifying authority. In the event of a 'hit', the second step is to obtain access to each individual system that contains the matching data through the procedure prescribed for each database.[122] Finally, the MID will use the alphanumeric data stored in the CIR and the SIS II to detect multiple identities; it will create links between identical data to indicate whether the individual is lawfully registered in more than one system or whether identity fraud is suspected.[123]

---

Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399, Regulation (EU) 2017/2226, Regulation (EU) 2018/XX [the ETIAS Regulation], Regulation (EU) 2018/XX [the Regulation on SIS in the field of border checks] and Regulation (EU) 2018/XX [the eu-LISA Regulation]" COM(2018) 478 final.

[118] Regulation 2019/817 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA [2019] OJ L135/27; Regulation 2019/818 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 [2019] OJ L135/85 (Interoperability Regulations).

[119] Arts6-11 of Interoperability Regulations.

[120] Arts12-16 of Interoperability Regulations.

[121] Arts17-24 of Interoperability Regulations.

[122] Art.22 of Interoperability Regulations.

[123] Arts25-36 of Interoperability Regulations.

**Surveillance of Third-Country Nationals, Privacy and Data Protection: A Balance Rightly Struck?**

*A Concise Typology of Privacy and Data Protection Standards*

Personal data processing through databases inevitably raises questions regarding the protection of the right of third-country nationals to private life, as enshrined in Article 8 European Convention on Human Rights (ECHR) and Article 7 EU Charter of Fundamental Rights (EUCFR), and personal data protection as encompassed in Article 8 EUCFR.[124] Both rights are not absolute and may be limited pursuant to Article 52(1) EUCFR, provided that the limitations are provided for by law, genuinely meet an objective of general interest to the EU, safeguard the essence of the rights and respect the principle of proportionality. Perhaps unsurprisingly, the proliferation of databases has not been accompanied by a substantial privacy assessment by the EU Court of Justice, presumably due to lack of awareness of or interest in the privacy issue, given the other more pressing rights at stake, such as non-refoulement.

Be that as it may, there is significant jurisprudence on surveillance practices at the national and EU levels. The systematic collection and storage of personal data has been repeatedly found to constitute an interference with the right to private life, irrespective of whether the data will be further used, or the collection took place in an intrusive manner.[125] A central consideration has been whether the personal data processing "taken as whole" allows for precise conclusions to be drawn on the private lives of the individuals affected.[126] Retention of biometric identifiers has been singled out as "not inconsequential, irrelevant or neutral".[127] Furthermore, the transmission of data to, and subsequent use by, other public authorities is considered a separate interference with the right to privacy since it expands the group of individuals with knowledge of the personal data.[128]

---

[124] See also Article 16 TFEU. The relationship between the two rights has been the subject of extensive debate. The view taken here is that the right to personal data protection safeguards and reinforces the right to private life, rather than replaces it. For an analysis see Vavoula, *Immigration and Privacy in the Law of the EU*, Ch.1.

[125] *Amann v Switzerland* (2000) 30 EHRR 843; *Rotaru v Romania* (2000) 8 BHRC 43.

[126] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (C-293/12 and C-594/12) ECLI:EU:C:2014:238, para.27; T*ele2 Sverige AB v Post-och Telestyrelsen, and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis* (C-203/15 and C-698/15) ECLI:EU:C:2016:970, para.99; Opinion 1/15 ECLI:EU:C:2017:592, para.150.

[127] *S and Marper v UK* (2009) 48 EHRR 50, para.84. Also see *Schwarz v Stadt Bochum* (C-291/12, ECLI:EU:C:2013:670.

[128] *Weber and Saravia v Germany* (2008) 46 EHRR SE5.

With regard to proportionality, in *Digital Rights Ireland* and *Tele2*, the EU Court of Justice condemned generalised surveillance – a practice which "is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance'.[129] Therefore, the Court found the indiscriminate collection of personal data without any differentiation, limitation or exception to be unlawful.[130] Rather, the Court held that data collection must be confined to situations that pose a threat to public security – restricted to a time period, a geographical zone, groups of persons likely to be involved in a serious crime, or more broadly persons whose communications may contribute to law enforcement.[131] In Opinion 1/15, the transfer of PNR data by air carriers and their subsequent use by Canadian authorities was accepted as an appropriate instrument for the purpose of fighting terrorism and other serious crimes.[132]

As regards biometrics, in *S and Marper*, the ECtHR held that the retention of biometrics in connection with persons who are unsuspected of a criminal offence may lead to discrimination and stigmatisation and may undermine the presumption of innocence.[133] Furthermore, in *Schwarz* concerning the storage of two fingerprints in EU biometric passports, the EU Court of Justice stressed the impact on the individual both in terms of the possibility of a false match (between the fingerprints of the passport holder and the fingerprints in the passport) and as regards the registration of fingerprint data *per se*. The Court found that storage of these fingerprints in a medium, such as the passport, is proportionate, as it remains with their owner[134] and the fingerprints are used for verification purposes.[135] A possible mismatch would merely draw the attention of authorities to that person, resulting in a more detailed check in order to establish their identity.[136]

*Ex post* access must be restricted to what is strictly necessary, respect procedural and substantive conditions, and be limited to the purposes of preventing, detecting and prosecuting terrorist offences and other serious crimes.[137] In *Zakharov v Russia*, the ECtHR took the view that surveillance was lawful and proportionate only if based on reasonable suspicion, understood as

[129] *Digital Rights Ireland*, para.37.
[130] *Digital Rights Ireland*, para.57; *Tele2*, paras.105–108; *Maximillian Schrems v. Data Protection Commissioner* (C-362/14) ECLI:EU:C:2015:650, para.93.
[131] *Maximillian Schrems*, para.93.
[132] Opinion 1/15, paras186–189.
[133] *S and Marper*, para.122.
[134] *Schwarz*, para.48.
[135] *Schwarz*, para.56
[136] *Schwarz*, para.43.
[137] *Digital Rights Ireland*, paras60–62; *Tele2*, para.115.

> "factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures".[138]

In addition, the ECtHR found that access to data should be subject to prior review by a court or independent administrative body entrusted with ensuring compliance with constitutional and legislative limits on data processing.[139]

Moreover, retention periods should be limited on the basis of the data's potential usefulness and should remain as short as possible.[140] In Opinion 1/15 on the EU-Canada PNR Agreement the Grand Chamber distinguished between different situations: the transfer and storage of PNR data prior to (and for the purpose of) the entry into Canada; further use and storage during the passenger's stay; and the retention of PNR data after his or her departure. Whereas storage before entry was found to be proportionate,[141] the use of data during the stay had to be based on new circumstances and objective evidence.[142] Importantly, after departure, passengers subject to entry and exit checks should be regarded as "not presenting, in principle, a risk" for terrorism and serious crime. Once a passenger leaves Canada, therefore, there is no prima facie connection – not even indirect – between their PNR data and the objective of the agreement (fighting terrorism and serious crime) that would justify retaining the data.[143] Consequently, continued storage of all air passengers' data after departure is not justified and only in specific cases, on the basis of objective evidence, is storage of certain passengers' data.[144]

*The Case of Databases*

The standards analysed are applicable in the operation of databases for immigration control purposes and, even more, to the use of their data by law enforcement authorities. The personal data contained reveal very specific information about the private lives of individuals – regarding their travel habits, their personal status, possible personal associations, in the case of the VIS, and even their educational and occupational background, in the case of the ETIAS. The following section unpacks key privacy concerns by providing paradigmatic examples from the various databases on the issues of the necessity of specific information

[138] *Zakharov v Russia* (2015) ECHR 1065, para.260.
[139] *Digital Rights Ireland*, para.62; *Tele2*, para.120; In Opinion 1/15, the EU Court of Justice even stated that such review is "essential" (para.202).
[140] *S and Marper*, para.119; *Digital Rights Ireland*, paras63–64.
[141] Opinion 1/15, paras197–198.
[142] Opinion 1/15, paras199–202.
[143] Opinion 1/15, paras204–208.
[144] Opinion 1/15, paras204–208.

systems, the personal scope of such systems, the categories of personal data collected, the retention periods foreseen and the law enforcement access granted.

Necessity Revisited: "Mind the (Informational) Gap"

A key issue underpinning the operation of databases is whether their initial establishment and subsequent configurations are necessary in relation to the purposes pursued. Whereas the EU Court of Justice has so far not questioned the necessity of surveillance mechanisms, with prime examples being the invalidation of the Data Retention Directive and the rejection of the draft EU-Canada PNR Agreement,[145] the case of databases differs due to the complementarity and potential overlap between the purposes, personal scope and functions of databases as well as the function of databases as transplanting surveillance methods into the realm of immigration law, which is part of administrative law.

A primary example of how necessity of maintaining a database is debatable is the operation of Eurodac as a support mechanism for an arguably ill-functioning Dublin system.[146] Although Eurodac's initial establishment was not unnecessary,[147] it is broadly accepted that the Dublin system is not currently 'working' for either asylum seekers or Member States. On the one hand, asylum seekers are not deterred from defying the Dublin rules and moving on to Member States in the EU core, to seek decent reception conditions and to lodge their asylum applications.[148] On the other hand, both the EU Court of Justice[149] and the ECtHR[150] have released landmark rulings condemning appalling reception conditions, leading to the halt of transfers to Greece in view of its systemic deficiencies. Furthermore, available statistics demonstrate that during the period 2008–2012, only around 25% of outgoing requests resulted in transfers, meaning that Dublin transfers take place in only around 3 per cent of all European asylum cases.[151] In light of this, the failings of Dublin have a domino effect on the operation of Eurodac, stripping away its necessity, at least with its current modalities. Since the allocation mechanism is problematic and, therefore, must be

[145] *Digital Rights Ireland*, para.50.

[146] E. Guild et al., "New Approaches, Alternative Avenues and Means of Access to Asylum Procedures for Persons Seeking International Protection" (PE509.989, 2014).

[147] This pronouncement is with a caveat about the fingerprinting of irregular border crossers. See Vavoula, *Immigration and Privacy in the Law of the EU*, ch.4.

[148] On this issue, see among others, Jesuit Refugee Service, "Protection Interrupted: The Dublin Regulation's Impact on Asylum Seekers' Protection The DIASP Project" (2013); S. Fratzke, "Not Adding Up: The Fading Promise of Europe's Dublin System" (Migration Policy Institute, 2015).

[149] See for example, *NS v. Secretary of State for the Home Department and ME and Others v. Refugee Applications Commissioner and Minister for Justice, Equality and Law Reform* (C-411/10 and C-493/10) ECLI:EU:C:2011:865.

[150] *MSS v Belgium and Greece* (2011) 53 EHRR 2; *Tarakhel v Switzerland* (2015) 60 EHRR 28.

[151] Guild, "Moving the Borders of Europe", p.9. See also Commission, "Evaluation of the implementation of Dublin III Regulation – Final Report" (DG-Home, 2016), pp.56–57.

fundamentally reformed, the need for maintaining the instrument assisting in this allocation, namely Eurodac, must also be questioned. It is recalled that the function of Eurodac is tied to the operation of the Dublin system, therefore, though fingerprints of irregular migrants are also included, this is merely a necessary corollary stemming from the Dublin criteria for allocation of responsibility for an asylum claim. Consequently, the initial and traditional purpose of Eurodac is related to the administration of asylum law and not the identification of irregular migrants through fingerprinting or the fight against irregular migration more generally. In the light of this, the refurbishment and reconceptualisation of Eurodac as a tool for 'wider migration purposes' is questioned and it could be argued that this tweak has been promoted in order to disentangle the system from its asylum origins and thus legitimise its existence in view of the challenges surrounding the operation of the Dublin system.

Furthermore, the added value of establishing the EES and the ETIAS as new databases monitoring the movement of almost all foreign travellers is not evident, particularly in light of the operation of the VIS, which was only fully rolled out worldwide in 2016.[152] Whether the EES will tackle the issue of overstayers is highly uncertain: the information mechanism envisaged does not signify that the person is necessarily an overstayer, as there may be other reasons why a person has not exited properly, e.g. human error, illness, application for asylum, death.[153] Importantly, national authorities will not have further information as regards the whereabouts of the person in question.[154] Whereas the abolition of stamping and the modernisation of border controls will indeed be attained through the EES, it is debatable whether this justifies the creation of a large-scale database with millions records that may be used for a series of purposes. Besides, functional difficulties may also be experienced, questioning the appropriateness of a system as well; the example of the US IDENT system (formerly US-VISIT), on which the EES has been based, is illustrative in this context; years after its operationalisation, the matching of entry and exit records is not possible, as the biometric exit capability is still under development, which, in turn, nullifies the system's function to identify potential overstays.[155] Moreover, the necessity of the ETIAS has been based on the perceived risk posed by visa-exempt travellers, without, however, substantiating the existence of that risk. The lack of an impact assessment prior to the adoption of the proposal and the pre-2015 decision to discard the project are testaments of the

[152] V. Mitsilegas, *The Criminalisation of Irregular Migration in Europe: Challenges for Human Rights and the Rule of Law* (Dordrecht: Springer, 2015), p.34.
[153] B. Hayes and M. Vermeulen, "Borderline – The EU's New Border Surveillance Initiatives" (Heinrich Böll Stiftung 2012), p.41.
[154] Meijers Committee, "Note on the Smart Borders Proposals" (CM1307), p.2.
[155] A considerable amount of reports by the Government Accountability Office (GAO) have been released in this respect. For the most recent one see GAO, "DHS Has Made Progress in Planning for a Biometric Air Exit System and Reporting Overstays, but Challenges Remain" (2017).

logic underpinning this field:[156] fill any and all "information gaps", rather than address clear evidence-based operational needs. This rather follows an approach whereby all third-country nationals are essentially treated as representing security risks, of variant gradation –hence the discrepancies in the respective legal bases-, which necessitates the monitoring of their movement and actions. In this logic, necessity is based on data greediness, technological availability and an evolving understanding of travel as an *a priori* suspicious activity performed by risky individuals that legitimises the intervention of the EU as a norm creator. The new generation of databases is thus being created with a view to completing, through systematic personal data processing, the "puzzle" of third-country nationals interacting with the EU in any way, be it administrative or law enforcement.

Personal Scope

The puzzle approach to databases is evident in the personal scope of databases. A key example of the EU's sweeping monitoring of third-country nationals, irrespective of proportionality considerations, is the grounds for entering alerts in the SIS II. In the first years of operation of the system, it was estimated that 77% of alerts were entered for the wrong reasons, raising questions of procedural fairness in SIS decision-making.[157] Similarly, the decision to register irregular migrants in the SIS rested entirely within the discretion of national authorities, resulting in significant discrepancies in the implementation.[158] Certain Member States, Germany and Italy in particular, were more rigorous in inserting alerts[159] and, therefore, third-country nationals faced differential treatment depending on the State in which they were found to be irregularly entering or staying. Over time, efforts to harmonise the recording of alerts stepped up, but divergences still persist.[160] In certain Member States the threshold for entering alerts is significantly higher than in others. For instance, in Lithuania, the refusal or annulment of a visa and the refusal or withdrawal of a residence permit triggers a SIS II alert, whereas in other Member States the categories set out in the Regulation are followed and in numerous States a return decision is automatically accompanied by an alert. [161] The mandatory registration of entry bans and return decisions in the refurbished SIS II will

[156] See Alegre, Jeandesboz, and Vavoula, "European Travel Information and Authorisation System (ETIAS): Border Management, Fundamental Rights and Data Protection", p.27.
[157] S. Kabera Karanja, *Transparency and Proportionality in the Schengen Information System and Border Control Cooperation* (Leiden/Boston: Martinus Nijhoff, 2008), p.216.
[158] Brouwer, *Digital Borders and Real Rights*, pp.61–62.
[159] Schengen Joint Supervisory Authority, "Article 96 Inspection – Report of the Schengen Supervisory Authority on the Inspection of the Use of Article 96 Alerts in the Schengen Information System" (2013).
[160] See Vavoula, *Immigration and Privacy in the Law of the EU*, Ch.2.
[161] European Migration Network, "Ad Hoc Query on Procedures for Entering Foreigner's Data into the Schengen Information System" (2014) http://ec.europa.eu/dgs/home-affairs/what-we-

signify a further watering down of the SIS II standards and will lead to automatic storage of personal data of essentially all irregular migrants irrespective of how serious the violation of immigration law. By inclusion of this data, registration in the SIS II becomes unavoidable, even in cases when the individual has voluntarily left the national territory, which is disproportionate in view of the personal conduct of the person concerned. The proportionality criterion for the registration of alerts is thus nullified, substituted by race-to-the-bottom harmonisation.

The expansive approach to personal scope, this time explicitly linked to security concerns, is also illustrated by the proposal to expand the VIS to include holders of residence permits, residence cards and long-stay visas. In the VIS reform, the inability to verify the identity and documentation of these categories of persons against a centralised system is framed as a potential threat to the security of one of the Member States.

The Foucaultian 'Panopticon' metaphor -particularly popular in discussions about mass surveillance- is useful to comprehend the effects of information systems.[162] In essence, the creation of massive digital catalogues enable domestic authorities to *see* all different groups of third-country nationals. The eagerness to cover 'blind spots' and 'information gaps' so that everyone could be *seen* fits well with the analogy.[163] Each database on its own constitutes a means of establishing visibility over a significant period of time that may even result semi-permanent registrations, for example, in cases of frequent travellers whose personal data are stored in the EES, or apply for authorisation via the VIS or the ETIAS. By seeing all third-country nationals the emerging Digital Panopticon Union is enabled to sort them out between *bona fide* and *mala fide* and assign levels of dangerousness and not only preventively exclude those unwelcome, but also to manage them on the national territory.[164] Even if individuals may have undergone checks prior to their departure or at the border, their ongoing registration in massive databases, which may be processed for a variety of purposes, not necessarily related to the procedure for which their data is initially collected, indicates that the a permanent cloud of suspicion surrounds third-country nationals. As such, the Union is able to exert significant power on a vast majority of the non-EU population so that they are excluded from the territory and/or disciplined within. However, in an era of 'Security Union', whereby security and migration are fully intertwined the cloud of suspicion surrounds not only individuals who may have undergone a series of checks for obtaining legal

---

do/networks/european_migration_network/reports/docs/ad-hoc-queries/border/505_emn_ahq_procedures_entering_foreigners_data_into_the_sis__7jan2014_%wider_dissemination%29.pdf.

[162] M. Foucault, *Discipline and Punish – The Birth of Prison* (Paris: Editions Gallimard, 1975).

[163] For example see Commission, "Stronger and Smarter Information Systems for Borders and Security", pp.COM(2016) 205 final, p.2, 3, 5, 12 and 18.

[164] See the references to the work of Broeders and Bigo in the introduction.

documentation but also the Member States who granted the residence status, who can only trust each other if an EU technological fix intervenes.

Categories of Collected Information

The high volume of personal data collected in certain cases goes beyond necessity and proportionality. For example, in the VIS, a category of personal data that raises proportionality concerns is that of persons issuing an invitation or sponsoring the stay of a visa applicant, persons who may be EU citizens or third-country long-term residents. In the course of routine implementation of the EU visa policy, the processing of these data is excessive and disproportionate and may lead to the creation of a mini-register on the side. Furthermore, in light of law enforcement access to the VIS data, their registration and consultation raises further concerns, as their data may be used in police investigations. Another example of disproportionate collection comes from the ETIAS and the processing of data on the applicant's level of education; the US ESTA does not collect this category of information and it is unclear why the ETIAS needs to do so.

Furthermore, the routine storage of biometrics – a special category of personal data– [165] in all databases but the ETIAS is questionable. In contrast with the storage of fingerprints in biometric passports, as in *Schwarz*, in databases biometrics are stored centrally and therefore the individuals concerned may lose control of their personal data. Furthermore, when biometrics are centrally stored, the error rates are impacted by the number of persons contained in the system.[166] Therefore, the larger the system, the greater the probability of a 'hit' based on an error. In cases of large-scale databases holding millions of records, the possibility of a false match is enhanced, particularly if there are data quality issues.[167] Such an error can have severe consequences: the wrongful return of the individual to another Member State on the basis of Eurodac hit; refusal of entry into the Schengen area; or even implication of the person in criminal proceedings in the framework of law enforcement. In addition, given that the VIS – and the revised Eurodac, if agreed – includes a digital photo, the collection of

[165] Art.9 of Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (General Data Protection Regulation); Art.10, Directive 2016/680 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 or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.

[166] Kindt, *Privacy nd Data Protection Issues of Biometric Identifiers*, p.59.

[167] See Fundamental Rights Agency, :Fundamental Rights and the Interoperability of EU Information Systems: Borders and Security" (2017), p.30. As regards the SIS II see also Commission, "Report on the Evaluation of the SIS II", p.11.

fewer fingerprints would have sufficed for identification purposes, even though that would frustrate the ancillary purpose of the systems to assist in crime prevention or investigation.

Retention Periods

The period during which personal data must be retained is vital, as continued storage and use of data perpetuates the effects of the interference with the right to private life. In the case of Eurodac, the ten-year retention period for asylum seekers was never properly justified; even though the Parliament had suggested reducing it to five years, the amendment was ignored by the Council.[168] As for the current eighteen-month retention period for the fingerprints of irregular border crossers, it does not correspond to the one-year responsibility of Member States for asylum seekers under Dublin rules. Furthermore, in the case of the SIS II, broad leeway has been granted to Member States: the three-year rule for deletion of the data subject to review without any maximum retention period being imposed on the Member States. The current trend points to an emerging default retention period of five years; this default for all EU databases appears to be useful for the purposes of interoperability.

Importantly, in light of the Opinion 1/15, the EU's existing and proposed databases make no distinction between the different phases of a third-country national's journey. For example, both the EES and the ETIAS will continue to store personal data even after the departure of the individual concerned in order to serve immigration-control purposes. However, according to the CJEU case law, after the departure of travellers, storage is justified only in relation to certain individuals on the basis of objective evidence. Therefore, the premise of databases as systems which may encompass an array of purposes creates a paradox, whereby the continued storage of personal data of all individuals captured by the database may be justified for administrative purposes, but has a significant spillover effect because of law enforcement access to their data, and perpetuates the risk for the individuals concerned.

Law Enforcement Access

There are also a number of issues related to law enforcement access to databases for third-country nationals. As explained earlier, in the case of the SIS II, the interrelation between immigration control and law enforcement was pre-embedded in the structure of the system, which had no unitary and limited purpose. Even though its main preoccupation was and continues to be immigration control, a de facto mission creep into law enforcement has thus been evident. Furthermore, the ECRIS-TCN is a law enforcement tool aimed at enabling Member States to exchange criminal records on third-country nationals. With regard to the

[168] Aus, "Eurodac: A Solution Looking for a Problem".

remaining databases, law enforcement access is an ancillary purpose, an add-on to the overarching functions of the system and as such, for the time being, such consultation may take place under specific circumstances only. Nevertheless, it must be stressed that law enforcement access is not obvious[169] and compelling evidence justifying the addition of this purpose must be adduced. As with the necessity of setting up the databases in the first place, justification of the need for law enforcement access has often been fragile.[170] Furthermore, the Eurodac example clearly illustrates the inherent danger of mission creep when personal data is centrally stored: once information is stored for a specific purpose, there is a real possibility of the system being re-purposed for objectives that were not initially contemplated.

As for the modalities of law enforcement access, these substantially fall short of the standards set out by the European Courts.[171] Whereas no routine access is foreseen, a series of loopholes remain. The national authorities allowed to consult the data are those responsible for the prevention, detection and investigation of terrorist offences or of other serious criminal offences as designated at the national level. As is evident from this expansive definition, national governments have considerable leeway to designate a wide array of agencies. There is no other guidance, requirement or limit contained in the EU legal instruments. Indeed, national intelligence agencies may also be given access if the Member State so chooses; only in the case of Eurodac have intelligence services been explicitly excluded.[172] The inclusion of intelligence services is worrisome; although it is to be welcomed that they are bound by the same rules as the rest of national authorities,[173] their operation is obscure when compared to police agencies. Once a Member State determines which authorities are to be given law enforcement access, the list of designated authorities is communicated to the Commission and published in the Official Journal, but there is no EU-level control and oversight. Finally, with regard to the procedure for consulting the data, in all cases, the designated authorities must submit a reasoned electronic request to an authority (Central Access Point or in the case of Eurodac to a Verifying Authority) that ascertains that the conditions for obtaining access have

[169] As is demonstrated by the fact that in designing the EES, the Commission initially left out law enforcement, and a proposal for recasting the Eurodac Regulation, including law enforcement access to asylum seekers' data, was blocked by the European Parliament in 2009.

[170] For the case of Eurodac see N. Vavoula, "The Recast Eurodac Regulation: Are Asylum Seekers Treated as Suspected Criminals?" in C. Bauloz et al. (eds), *Seeking Asylum in the European Union: Selected Protection Issues Raised by the Second Phase of the Common European Asylum System* (Leiden: Brill, 2015), p.260.

[171] For a detailed analysis see N. Vavoula, "The Use of European Centralised Databases for Third-Country Nationals as Law Enforcement Weapons in the Fight against Impunity" in L. Marin and S. Montaldo (eds), *The Fight Against Impunity in EU Law* (Oxford: Hart, forthcoming 2020).

[172] Art 5(1) of the recast Eurodac Regulation.

[173] European Data Protection Supervisor, "on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (COM(2004)835 final)" [2005] OJ C181/13.

been met. Nevertheless, this procedure is not in line with the criteria set out in *Digital Rights Ireland, Tele2*, and Opinion 1/15, where the EU Court of Justice explicitly required that law enforcement access to the data be made dependent on prior review carried out by a court or by an independent administrative body. Considering that requesting and verifying authorities may be part of the same law enforcement agency, the independence and objective judgment of the necessity of access may be jeopardised.

Interoperability: The Glue that Binds them All

With the operationalisation of interoperability, the landscape of information systems will be forever changed. Whereas it has been correctly pointed out that interoperability will not frustrate existing limits on access rights of national authorities, it must be highlighted that the use of personal data will be attached to new purposes, which are not to be found in the respective legal instruments. For instance, Eurodac data will be used to detect persons with multiple identities even though Eurodac's mandate does not specify this use. Another worrisome change involves the possibility for a Member State police authority to query the CIR with the biometric data of a person over the age of 12 taken during an identity check in presence of that person, for the sole purpose of identifying them.[174] Regrettably, the Regulations do not envisage common criteria[175] or limitations as regards their frequency and intensity may lead to highly divergent rules and practices at the national level, whereby third-country nationals, or EU nationals looking like foreigners, may find themselves being subjected to different practices depending on how proactive a police authority in a Member State is. As noted by the Article 29 Working Party (now European Data Protection Board): "querying the CIR … could result in a very large number of accesses given the volume of identity checks led by police authorities".[176] Extensive identity checks by police authorities may fuel discriminatory practices based on increased suspicion towards specific categories of individuals, which may proceed to identification checks to third-country nationals on the spot solely on the basis of extensive (racial) profiling.[177]

Importantly, interoperability involves the masked setting up of new databases based on combining data from different sources – the BMS,[178] the CIR and the MID.[179] The fancy

[174] Art.20 of the Interoperability Regulations.

[175] EDPS, Opinion 4/2018 (16.04.2018), pp.12-13.

[176] Article 29 Working Party, "Opinion on Commission proposals on establishing a framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration" (WP266, 2018), p.11.

[177] T. Quintel, "Interoperability of EU Databases and Access to Personal Data by National Police Authorities under Article 20 of the Commission Proposals" (2018) 4 *European Data Protection Law Review* 470.

[178] The BMS will store templates of biometric data, which is uncertain as to whether they constitute personal data. On the reasons to the affirmative see N. Vavoula, "Interoperability of EU Centralised

wording that is used ("component" and "repository")[180] should not distract from the dangerous reality of massive catalogues of third-country nationals at EU level. The aggregation of data through databases signifies a new information-processing paradigm of mass and indiscriminate surveillance. By combining information from different systems, authorities are empowered to draw more precise conclusions on the private lives of individuals. It is not far-fetched to characterise interoperability as a decisive step towards a single EU information system in the service of an EU Big Brother.[181] The CIR in particular is highly problematic; whilst each database *on its own* may not qualify as establishing generalised and indiscriminate surveillance pursuant to Opinion 1/15, because it involves only a fraction of third-country nationals, the CIR as a new database combining materials from the underlying systems ticks all the boxes to be considered as unlawful mass surveillance. The lack of connection with the SIS II does not alter the fact that all categories of third-country nationals will be captured by the CIR, as that system includes alerts on irregular migrants and criminals, which are already captured by Eurodac and ECRIS-TCN respectively. Interoperability will thus enable domestic authorities to enhance such visibility and *know* all the different categories of third-country nationals better, by assembling records from the different systems and combine the different personal data to create richer profiles regarding their movement and administrative or criminal procedures that they have undergone. Moving beyond its traditional understanding, as explained above, the "pan-opticon" (coming from the ancient Greek "πάν" (all) + "οπτικόν" (of sight)) is progressively replaced by the "pan-gnosticon" ("πάν" (all) + "γνωστικόν" (of knowledge), an emerging know-it-all surveillance system, whereby authorities would be able to achieve total awareness of the identities and movements of the individuals, with the ultimate aim of preventing, deterring, controlling, or in more neutral words "managing" people.

Another key change brought about by interoperability involves law enforcement access to third-country nationals' data. Although, as mentioned previously, access is currently reserved for specific cases based on the necessity of consulting the data, interoperability marks a significant step towards routine access. The Interoperability Regulations envisage a two-step approach, in which designated authorities shall first check all systems through the CIR on a hit/no hit basis and then, if they get a hit, satisfy the conditions applicable to each of the underlying databases to obtain access to the individual data pots. Yet even just a hit is

---

Databases for Third-Country Nationals: The Deathblow to their Privacy and Data Protection?" (*European Public Law*, forthcoming 2020).

[179] However, the MID will not store personal data.

[180] For example, see Interoperability Proposals, p.7.

[181] T. Bunyan, "The Point of No Return - Interoperability Morphs into the Creation of a Big Brother Centralised EU State Database Including All Existing and Future Justice and Home Affairs Databases" (Statewatch, May 2018), p.10.

significant since it reveals elements of an individual's personal life, for instance that they are visa free travellers, and therefore the first step of checking whether there is personal data should be covered by the conditions of access.[182] Importantly, it is hard to believe that upon finding that a database holds information on a person, the verifying authority ensuring the conditions for access have been met will not allow such access. In other words, not only the independence and objectivity but also the very existence of a verifying authority may be biased by the two-step approach.

Overall, interoperability negates the relevance of the purpose limitation principle by essentially enabling databases to be used for almost any purpose as long as this is not incompatible with the original purpose for which the data have been originally collected. The multiple reconfigurations of the systems over time denote that the threshold for such "incompatibility" is impossible to reach and the limits of these systems are far from being exceeded. This logic does not correspond to the traditional understanding of migration control, but rather fosters, validates and accentuates the transformation of databases for third-country nationals to "security systems" their reconceptualisation as quasi-intelligence tools.[183]

**Conclusion**

The aim of this article has been twofold: to map the evolution of EU-wide databases for third-country nationals and to highlight a series of privacy and data protection concerns that have been triggered by their establishment, operation and reconfiguration over time. Through the systematic categorisation of EU information systems in three distinct eras, it has been demonstrated that their operation entails the collection and storage of a wide range of personal data, including biometrics, and their further processing for multiple and often diverging purposes, which are anything but fixed. In the future, driven by the logic of closing information gaps, lack of EU citizenship will entitle State authorities to require individuals to provide extensive personal data, including sensitive data. The big picture is that of systematic expansion of the personal scope of EU databases: once the aforementioned systems are fully operational, almost no third-country national will be left un-surveilled through at least one database. Apart from expanding the groups of individuals concerned and the purposes and the categories of data to be collected, the initial compartmentalised approach has been abandoned in favour of interoperability, enabling the data pots to interact. The aggregation of data will

[182] T. Quintel, "Connecting Personal Data of Third Country Nationals: Interoperability of EU Databases in the Light of the CJEU's Case Law on Data Retention" (University of Luxembourg Law Working Papers, March 2018), p.16; EDPS, Opinion 4/2018, p.17.

[183] See N. Vavoula, "Interoperability of European Centralised Databases: Another Nail in the Coffin of Third-Country Nationals' Privacy?" (EU Immigration and Asylum Law and Policy, 08.07.2019) http://eumigrationlawblog.eu/interoperability-of-european-centralised-databases-another-nail-in-the-coffin-of-third-country-nationals-privacy/ (accessed 8 October 2019).

not only generate new databases and new data (MID) but will also transform existing databases into powerful intelligence tools.

These trends have utterly blurred the boundaries between immigration and criminal law. They had been driven by, and will in turn feed, the perception of third-country nationals as potential risks for EU internal security, and have significant repercussions for their privacy and data protection. This article has provided concrete examples of disproportionate data processing by scrutinising the operating rules of the many databases, as well as their interoperability, against the jurisprudential benchmark of the European Courts. The necessity of information systems has been taken for granted rather than robustly justified; the existence of the old generation of databases has generated a domino effect, in which their operational flaws are used to justify the new and revised systems. Furthermore, specific categories of information should not be available to certain authorities. With the routine registration of biometrics, the provision of extensive retention periods and the use of data for law enforcement purposes, the administration of third-country nationals through electronic databases has progressively been transformed into a system of mass surveillance. Particularly in the VIS, the EES and the ETIAS, everyday legitimate activities are monitored.[184] Travel has emerged as an inherently dangerous activity and mobility operates as a trigger for state surveillance.

With surveillance of movement becoming the norm, a key question remains: will it expand to EU nationals, undermining not only their privacy but also EU citizenship rights? This is more than a rhetorical question, as the cases of the EES and the ECRIS-TCN suggest. These examples confirm the dystopian predictions that the new technologies are being tested on foreigners so that they can then be extended to EU nationals. In an era when every third-country national is potentially a risk justifying security surveillance, the divide between the privacy safeguards for EU and third-country nationals will become acute. Might, in the future, the standards of privacy protection for EU nationals be lowered to close this gap? It remains to be seen what the future will bring to the ongoing battle between security and privacy.

[184] See D. Lyon, *Surveillance Society: Monitoring Everyday Life* (Buckingham: Open University Press, 2001).