Finding the Balance between Security and Human Rights in the EU Border Security Ecosystem

Elrick, Lauren

Published in:
European Journal of Law and Technology

Publication date:
2021

Citation for published version (APA):
Elrick, L. (2021). Finding the Balance between Security and Human Rights in the EU Border Security Ecosystem. *European Journal of Law and Technology*, *12*(1), 1-42.

European Journal of Law and Technology, Vol 12 No.1 (2021)

EJLT European Journal of Law and Technology

Finding the Balance between Security and Human Rights in the EU Border Security Ecosystem

Lauren E. Elrick*

Abstract

In order to address the *'complex landscape'* of large-scale information systems which have developed within the fields of migration and security, the European Union adopted two Regulations on Interoperability (Reg (EU) 2019/817 and Reg (EU) 2019/818) on the 20th May 2019. These twin Regulations establish a framework composed of four components: firstly, a European Search Portal (ESP); secondly, a Shared Biometric Matching Service (BMS); thirdly, a Common Identity Repository (CIR); and fourthly, a Multiple-Identity Detector (MID).

Through these components, the EU seeks to close information gaps which exist between the various information systems, enabling the different systems to supplement each other. The EU argues that doing so helps to ensure the correct identification of individuals presenting themselves at an EU border, and assists in achieving a number of aims such as improving the effectiveness of external border checks, preventing illegal immigration and contributing to a high level of security within the Area of Freedom, Security and Justice.

While beneficial from the standpoint of simplifying data exchange, these Regulations raise significant human rights concerns, particularly in relation to privacy and data protection. Through considering this *'complex landscape'* through a holistic perspective, this article considers whether rather than simplifying how the information within these databases are accessed, the Interoperability Regulations, in fact, further complicates it, by failing to take into account the importance of the respective purposes behind each individual database.

As an ecosystems approach highlights, rather than looking at the interoperability provisions in isolation, greater attention should be paid to the wider context within which these databases have developed. It is suggested that by ignoring this context, these

[*] Security, Technology and e-Privacy (STeP) Research Group, Faculty of Law, University of Groningen, The Netherlands and 'Mihai Viteazul' National Intelligence Academy, Romania.
ORCID: https://orcid.org/0000-0003-4458-9745

Regulations prioritise the development of new tools for security purposes at the expense of the human rights of migrants.

Keywords: Border Security; Human Rights; Europe.

1. Introduction

The last few decades have seen the field of border security[1] within the European Union (EU) undergo a revolution, largely motivated by fears that the lack of internal borders within the Schengen Area - one of the Union's defining features – leaves the territory of the Union open to exploitation from bad faith actors. In particular, concerns have arisen that if Member States do not have the ability to (a) accurately monitor who is within their territories at any one time, (b) prevent those who might pose a threat from entering in the first place and (c) monitor the status of those who have been ordered to leave, then the entire territory of the Union becomes vulnerable to attack.

Several high-profile terrorist attacks within the EU in recent years have re-emphasised these fears. In order to compensate for this, there has been an increased drive to strengthen the external borders of the EU, leading to the progressive development of what Vavoula has termed a *'mille-feuille'* of large-scale information systems within the fields of migration and security.[2] The foundations of this began with the development of the Schengen Information System (SIS) (since replaced with the updated SIS II) in the mid-

[1] In his 'State of the Union 2016' address, the then President of the European Commission, Jean-Claude Juncker identified border security as one of the main priorities of his Commission. Similarly, the EU's most recent Security Union Strategy recognises that in order to address challenges common throughout the Member States of the European Union 'fully implement[ing] border security legislation and [making] full use of all relevant EU databases to share information on known suspects' was an important step. In light of these documents, this article therefore uses the term 'border security' to refer to the entire security complex surrounding the protection of the EU's borders, encompassing the protection of the external borders, migration management, combatting internal security threats and preventing cross-border crime. See, Jean-Claude Juncker, *State of the Union 2016* (European Commission 2016), 62; European Commission, 'A Step-Change in Migration Management and Border Security' (2019) <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-migration/20190306_managing-migration-factsheet-step-change-migration-management-border-security-timeline_en.pdf> accessed 23 February 2021; European Commission, 'Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy' COM(2020) 605 final, 17. For a more detailed consideration of how the concept of border security concept has developed at the EU level, *see* Valsamis Mitsilegas, 'Border Security in the European Union: Towards Centralised Controls and Maximum Surveillance' in Annaliese Baldaccini, Elspeth Guild and Helen Toner (eds), *Whose Freedom, Security and Justice? EU Immigration and Asylum Law and Policy* (Hart Publishing, 2007); and Annaliese Baldaccini, 'Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases' (2008) 10 European Journal of Migration and Law 31.

[2] Niovi Vavoula, 'Databases for Non-EU Nationals and the Right to Private Life: Towards a System of Generalised Surveillance of Movement?' in Francesca Bignami (ed), *EU Law in Populist Times: Crises and Prospects* (Cambridge University Press 2020), 229.

1990s as a compensatory measure for the abolition of internal border checks within the Schengen Area.

This was soon followed by the introduction of the European Dactyloscopy (more commonly referred to as Eurodac) to record and process the fingerprints of asylum seekers and irregular border-crossers in order to fulfil the requirements of the Dublin System. Thereafter came the Visa Information System (VIS). This allowed for the faster exchange of information on visa applicants. More recently, legislation has been adopted to supplement these with three new systems: the Entry-Exit System (EES) which will register whenever a third country national (TCN) crosses the EU's external border; the European Travel Information and Authorisation System (ETIAS) which will implement a pre-travel screening system for visa-exempt travellers, and the European Criminal Records Information System – Third Country Nationals (ECRIS-TCN) which will enable Member States to exchange criminal records on non-EU nationals who have been convicted of an offence within a Member State.[3]

This has resulted in the creation of a network of databases operating within the border security field, each of which stores a separate set of information and which are *'rarely interconnected.'*[4] This has been described as creating a *'complex landscape'*[5] of differently governed information systems within the field of borders, security and migration management. This currently siloed structure primarily resulted from the fact that each of these databases developed within their own distinct institutional, legal and political context - a decision premised on the desire to protect the fundamental rights of the TCNs whose data would be collected within these systems.[6]

However, this siloed structure also makes it difficult to share information between the systems.[7] In addition, several other shortcomings have been identified including: (i) sub-optimal functionalities in the existing systems; (ii) gaps in the EU's data management architecture; and (iii) a particularly fragmented architecture within the field of border control and security.[8] Consequently, the past few years have seen a number of proposals

[3] A similar de-centralised system, the European Criminal Records Information System (ECRIS) was established in 2012. However, this system only allows Member States to exchange criminal record information regarding EU nationals. For non-EU nationals, Member States are forced to contact each individual Member State in order to find out whether any hold conviction information on a specific national. The creation of the ECRIS-TCN is therefore designed to establish a similar system for the exchange of criminal record information on third country nationals as already exists for EU nationals through the ECRIS system.

[4] European Commission, 'Communication from the Commission to the European Parliament, and the Council: Stronger and Smarter Information Systems for Borders and Security' COM(2016) 205 final, 3.

[5] *Ibid*.

[6] Mijja Gutheil et al, 'Interoperability of Justice and Home Affairs Systems, Study on Behalf of the European Parliament' (LIBE Committee 2018) PE.604.947 <https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604947/IPOL_STU(2018)604947_EN.pdf> accessed 19 May 2021.

[7] COM(2016) 205 final.

[8] *Ibid* 3.

made advocating the benefits of bringing these databases together within an interoperable framework.[9]

Ultimately, two Regulations establishing a framework for interoperability between EU information systems were adopted on the 20th May 2019: Regulation (EU) 2019/817 (in the field of borders and visas) and Regulation (EU) 2019/818 (in the field of police and judicial cooperation, asylum and migration).[10]

These Interoperability Regulations seek to address the previously identified issues by pursuing three objectives.

Firstly, strengthening and maximising the benefits of the existing information systems; Secondly, addressing information gaps through the establishment of new systems; Thirdly, enhancing interoperability between the systems.[11] It is hoped that by doing so it will ensure: (a) fast, seamless, systematic and controlled access for end-users; (b) combat identity fraud through enabling the detection of multiple identities using the same biometric data; (c) facilitate checks on third-country nationals; and (d) streamline access by law enforcement authorities (LEAs) to non-law enforcement information systems.[12]

However, the introduction of interoperability between these databases raises a number of issues, particularly in regards to the protection of human rights.[13] Most prominent is the

[9] COM(2016) 205 final; European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visas) 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' (Interoperability Proposal, Borders and Visas) COM(2017) 793 final; European 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)' (Interoperability Proposal, Police and Judicial Cooperation, Asylum and Migration) COM(2017) 794 final; European Commission, High-Level Expert Group on Information Systems and Interoperability, 'Final Report' (May 2017) <https://www.statewatch.org/media/documents/news/2017/may/eu-com-hleg-info-systems-interoperability-final-report-5-17.pdf> accessed 19 May 2021.

[10] Regulation (EU) 2019/817 of 20 May 2019 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 L 135/27; Regulation (EU) 2019/818 of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 [2019] OJ L 135/85.

[11] COM(2017) 793 final, 11; COM(2017) 794 final, 12.

[12] COM(2017) 793 final, 3; COM(2017) 794 final, 3.

[13] *See, for example*, Niovi Vavoula, 'Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?' (2020) 26(1) European Public Law 131; Teresa Quintel, 'Interoperable Data Exchanges Within Different Data Protection Regimes: The Case of Europol and the European Border and Coast Guard Agency' (2020) 26(1) European Public Law 205; Evelien Brouwer, 'Large-Scale Databases and Interoperability in Migration and Border Policies: The Non-Discriminatory Approach of Data Protection (2020) 26(1) European Public Law 71.

recognition that these measures have the potential to fundamentally alter the balance that exists between the authorisation of intrusive measures in order to achieve security related goals and the protection of fundamental rights. Privacy and data protection are already heavily restricted in border areas - a necessary corollary of the fact that identifying and preventing the entry of bad-faith actors requires being able to accurately identify every individual.

Yet, it is also important to consider the affect that interoperability will have on the rights of TCNs more generally. As will be seen below, through the development of each new database, the amount of information collected on this category of individuals substantially increases - showing how through a series of steps the migratory process has come to be distrusted and the unidentified migrant perceived as a security threat. This trend exemplifies the process which has come to be known as the *'securitisation of migration.'*[14][15]

Consequently, this has the potential to raise claims relating to non-discrimination and racial profiling, as well as the inadequate protection of data subject rights. This article will

[14] The concept of securitisation was introduced by Waever to describe the process through which ordinary objects and events come to be politicised as a security threat. In this way, they become recognised as a problem which the state has a right to defend themselves against. *See, for example,* Ole Waever, 'European Security Identities' (1996) 34(1) Journal of Common Market Studies 103 and Ole Waever, 'Securitization and Desecuritization' (1995) in Christopher W. Hughes and Lai Yew Meng (eds), *Security Studies: A Reader* (Routledge, 2011). This effect can be seen in relation to migration, whereby through securitisation the migrant (whether a refugee, asylum seeker or other category of immigrant, such as economic) comes to be identified as a threat to the security of the state. Once this process has occurred, it legitimises the use of rhetoric that additional measures can be used against these categories of individuals. For more information on how this process has occurred, *see* Jef Huysmans, 'The European Union and the Securitization of Migration' (2000) 38(5) Journal of Common Market Studies 751; Ariane Chebel d'Appollonia, *Frontiers of Fear: Immigration and Insecurity in the United States and Europe* (Cornell University Press 2012); Gabriella Lazaridis and Khursheed Wadia (eds), *The Securitisation of Migration in the EU: Debates since 9/11* (Palgrave Macmillan 2015); Valsamis Mitsilegas, Violeta Moreno-Lax and Niovi Vavoula (eds), *Securitising Asylum Flows: Deflection, Criminalisation and Challenges for Human Rights* (Brill Nijhoff 2020); Sarah Léonard and Christian Kaunert, 'The Securitisation of Migration in the European Union: Frontex and Its Evolving Security Practices' (2020) Journal of Ethnic and Migration Studies, DOI: 10.1080/1369183X.2020.1851469 and Valeria Bello, 'The Spiralling of the Securitisation of Migration in the EU: From the Management of a 'Crisis' to a Governance of Human Mobility?' (2020) Journal of Ethnic and Migration Studies, DOI: 10.1080/1369183X.2020.1851464.

[15] Within the EU, this process began with the abolishment of the internal borders of the Schengen Area, which stimulated the development of a range of policies aimed at controlling migration (Karamanidou 2015, 37), and ultimately led to the inclusion of immigration and asylum within regulatory frameworks designed to address security issues (Huysmans 2000, 753). *See, for example,* Lena Karamanidou, 'The Securitisation of European Migration Policies: Perceptions of Threat and Management of Risk' in Gabriella Lazaridis and Khursheed Wadia (eds), *The Securitisation of Migration in the EU: Debates since 9/11* (Palgrave Macmillan 2015), 37 and Huysmans (n 14), 753. The most important example of this can be found in the Convention Applying the Schengen Agreement 1990, through which immigration and asylum came to be connected with terrorism, border control and transnational crime (*see* Huysmans (n 14), 756). Following the 9/11 attacks, this process has intensified – *see, for example*, d'Appollonia (n 14) and Mikhail A. Alexseev, *Immigration Phobia and the Security Dilemma: Russia, Europe, and the United States* (Cambridge University Press 2006).

therefore seek to show how the introduction of an interoperable framework has only further complicated an already complex situation with regards to the protection of individual rights. It is proposed that what is required is a new method through which to consider this situation, one which enables a more holistic perspective to be taken. After all, while each individual database might be justifiable and proportionate on its own merits (a contestable point addressed further below),[16] when looked at from a holistic perspective, or taken as representing a cumulative threat to human rights, this might not be the case.

How can this be achieved? In nature, the concept of the ecosystem provides a method through which to understand and study the world. It recognises the existence of a closely interconnected system of actors, who are engaged in the exchange of information and resources. A key component of the ecosystem concept comes from the recognition that the non-living elements of the system have a crucial role to play in determining how the system operates. This article, therefore, considers the role that these large-scale IT databases – the non-living element of the border security ecosystem – play within the field of EU border security, and, in particular, whether the push for interoperability pursued by the EU actually helps to address the issue of complexity.[17]

Ultimately, this article considers how through utilising an ecosystems approach, it becomes clear that the EU's current way of thinking in regards to the use of large-scale information systems within the EU's border security field is fundamentally flawed.

2. Security versus human rights: migration as a security threat

In the post 9/11 period, migration has increasingly found itself tied together with terrorism. To quote Longo, the two issues have become wound together to represent a *'double-*

[16] *See, for example*, Niovi Vavoula, 'European Travel Information and Authorisation System (ETIAS): A Flanking Measure of the EU's Visa Policy with Far Reaching Privacy Implications' (2017) Queen Mary School of Law Legal Studies Research Paper No.256/2017 <https://ssrn.com/abstract=2928082> accessed 26 February 2021) on ETIAS; Vavoula (n 2) on Eurodac and Niovi Vavoula, 'Consultation of EU Immigration Databases for Law Enforcement Purposes: A Privacy and Data Protection Assessment' (2020) 22 European Journal of Migration 139 on EES); Chris Jones, 'Disproportionate and Discriminatory: The European Criminal Records Information System on Third-Country Nationals (ECRIS-TCN)' (Statewatch Analysis 2019) <https://www.statewatch.org/media/documents/analyses/no-340-ecris-tcn.pdf> accessed 26 February 2021 on ECRIS-TCN; Izabella Majcher, 'The Schengen-wide Entry Ban: How are Non-Citizens' Personal Data Protected?' (2020) Journal of Ethnic and Migration Studies, DOI: 10.1080/1369183X.2020.1796279 on the side effect of SIS alerts on the rights of TCNs; Willemijn Tiekstra, 'Free Movement Threatened by Terrorism: An Analysis of Measures Proposed to Improve EU Border Management' (International Centre for Counter-Terrorism, 2019), <https://www.jstor.org/stable/pdf/resrep19619.pdf?refreqid=excelsior%3A6fca15c364e9275b7d36bb3f464ae3ad> accessed 26 February 2021 on the EES, ETIAS and ECRIS-TCN; and Brouwer (n 13) and Vavoula (n 13) more generally on the issues of proportionality and necessity in relation to large-scale databases.

[17] For additional reading on this point, *see broadly* the works of Vavoula and Quintel cited throughout.

headed hydra of global mobility.'[18] Nonetheless, prior to the 9/11 attacks,[19] many Western States, both inside, and outside, of Europe, had started to view the presence of large numbers of migrants within their territories with mistrust.[20] Earlier attacks, such as the 1995 Paris Metro bombings, and attacks by the Kurdistan Workers' Party throughout Europe in the 1990s, had resulted in migrants being viewed with suspicion and seen as representing a potential security threat.[21]

However, the 9/11 attacks brought everything into a new light. Only weeks after the attacks, the United Nations Security Council adopted a resolution calling for States to *'prevent the movement of terrorists or terrorist groups by effective border controls and controls on issuance of identity papers and travel documents.'*[22] The attacks *'epitomized the worst fears related to immigration'*[23] and provided validation for a viewpoint that had increasingly been gaining momentum – that migrants could represent a safety and security threat to their citizens. This consequently legitimised the position that states could intervene and regulate their movement more closely. The movements of migrants – regardless of whether they were asylum seekers, refugees or economic migrants – were suddenly suspicious, their every motivation questioned.[24] They were no longer viewed from the standpoint of a welcome visitor, but rather as a potential enemy, waiting for the opportunity to attack and bring harm to their host state.[25] Their *'otherness'* made them dangerous – they were not bound by the same sense of shared community that a state's citizens were and as such their intentions towards the state could not be judged.[26] Thus, this meant that they needed to be closely watched and assessed in order to ensure that they did not pose a threat.

2.1 Immigration controls as counter-terrorism measures

Through a process of securitisation, immigration has therefore come to be perceived as a security threat.[27] This generalised fear and suspicion of immigrations has, over time, spilled

[18] Matthew Longo, *The Politics of Borders: Sovereignty, Security and the Citizen after 9/11* (Cambridge University Press 2018), 2.

[19] Indeed, as d'Appollonia (n 14), 51 notes, there is clear evidence that immigrants have been regarded with suspicion since at least the late eighteenth century.

[20] Fiona B Adamson, 'Crossing Borders: International Migration and National Security' (2006) 31(1) International Security 165; Baldaccini (n 1).

[21] Adamson (n 20), 165-166.

[22] United Nations Security Council, Resolution 1373 (28th September 2001), S/RES/1373, para 2(g).

[23] d'Appollonia (n 14), 50.

[24] Richard Perruchoud, 'State Sovereignty and Freedom of Movement' in Brian Opeskin, Richard Perruchoud and Jillyanne Redpath-Cross (eds), *Foundations of International Migration Law* (Cambridge University Press 2012); Adamson (n 20).

[25] Perruchoud (n 24); Michael Humphrey, 'Migration, Security and Insecurity' (2013) 34(2) Journal of Intercultural Studies 178; Lazaridis and Wadia (n 14).

[26] Richard W. Mansbach and Franke Wilmer, 'War, Violence and the Westphalian State System as a Moral Community' in Mathias Albert, David Jacobson and Yosef Lapid (eds), *Identities, Borders, Orders: Rethinking International Relations Theory* (University of Minnesota Press 2001); d'Appollonia (n 14).

[27] d'Appollonia (n 14); Lazaridis and Wadia (n 14); Léonard and Kaunert (n 14); Bello (n 14).

over and intermingled with fears regarding the growing threat of international terrorism. The beginnings of this process can be traced back to the 1980s, specifically the establishment of the Internal Market. When the Single European Act (SEA)[28] was signed in 1986, its objective was to advance political cooperation between the Member States, in order to achieve the goal of European unity.

It introduced several amendments to the Founding Treaties, one of which was the introduction of Article 8a to the Treaty of Rome (EEC). Through this, the Community agreed to work towards achieving the aim of establishing an area *'without internal frontiers in which the free movement of goods, persons, services and capital is ensured.'*[29] Almost immediately, concerns were raised about the effect that establishing free movement would have on the security of the European Community. Unlike the mobility of capital and goods which was identified as beneficial to European society, the mobility of people was constructed much more negatively.[30]

For instance, a meeting of the Heads of State and Governments of the Trevi Group (a multilateral forum established in order to enhance cooperation regarding counter-terrorism) on the 5-6th December 1986 was devoted to examining how to *'further intensify cooperation in the fight against terrorism, illegal immigration and drug trafficking'*[31] – three problems, they noted, which stem from the realisation of the right to free movement of people.[32]

European Community policies quickly began to reflect the view that in order to fully actualise the concept of free movement, there would have to be a strengthening of the external borders of the Community so as to counteract the effect of abolishing the internal borders.[33] As Huysmans notes, this was based on the reasoning that without such increased controls, the Community would be unable to *'guarantee a sufficient level of control of who and what can legitimately enter the space of free movement.'*[34]

Consequently, a range of *'compensatory measures'* were adopted in order to address the potential security risks created by abolishing the internal borders.[35] These included common policies regarding visas, asylum, and police and judicial cooperation.[36] What many

[28] [1987] OJ L 169/1.
[29] Art 13, [1987] OJ L 169/1**.**
[30] Didier Bigo, 'Criminalisation of 'Migrants': The Side Effect of the Will to Control the Frontiers and the Sovereign Illusion' in Barbara Bogusz, Ryszard Cholewinski, Adam Cygan and Erika Szyszczak (eds), *Irregular Migration and Human Rights: Theoretical, European and International Perspectives* (Martinus Nijhoff Publishers 2004).
[31] Tony Bunyan (ed), *Key Texts on Justice and Home Affairs in the European Union: Volume 1 (1976-1993) – From Trevi to Maastricht* (Statewatch 1997), 10.
[32] d'Appollonia (n 14); Bunyan (n 31).
[33] European Council, 'The Hague Programme: Strengthening Freedom, Security and Justice in the European Union' [2005] OJ C53/1; Baldaccini (n 1).
[34] Huysmans (n 14), 759.
[35] d'Appollonia (n 14); Vavoula (n 2).
[36] Sara Casella Colombeau, 'Policing the Internal Schengen Borders – Managing the Double Bind Between Free Movement and Migration Control' (2017) 27(5) Policing and Society 480; Morten

of these compensatory measures had in common was that they introduced increasingly stricter controls on immigration.

Over time, these immigration controls have increasingly come to be conflated with measures designed to combat the threat of international terrorism – a move largely stemming from the 9/11 attacks, but further reinforced by the attacks in Madrid in 2004 and London in 2005.[37] Many of the measures employed at the external border, such as collecting fingerprints, and other forms of biometrics, treat third country nationals not *'as individuals, but as risk categories.'*[38] While the primary justification behind the introduction of these technologies is to stem irregular immigration, they have increasingly also been identified for their security benefits.

Correspondingly, the data collected has progressively also been co-opted for the achievement of wider security-related purposes, such as countering terrorism. Data collected for immigration purposes, such as issuing a visa, or, granting asylum, can also be used to enable the identification of wanted or dangerous individuals and either stop them from entering the territory of the EU or to ensure that they are expelled.[39] In this way, border controls are turned into a method of risk assessment through which individuals are assessed against a range of criteria in order to ascertain the level of threat they pose.[40] However, it must be recognised that treating immigration data this way can lead to the gradual criminalisation of migrants.[41] Frequently these measures are justified on the grounds of necessity – after all, in order to prevent someone undesirable from entering the territory of the Union you need to be able to identify them accurately. In many cases, stopping them at the state border (a location where authorities have the potential to subject whomever they like to detailed checks) represents the clearest opportunity a state will have to do this.[42]

Consequently, in the post-9/11 period, there has been an increased drive to tighten immigration controls, justified on the important role these measures can play in countering

Jarlbæk Pedersen, 'The Intimate Relationship Between Security, Effectiveness, and Legitimacy: A New Look at the Schengen Compensatory Measures' (2015) 24(4) European Security 541.

[37] Sarah Le'onard, 'Border Controls as a Dimension of the European Union's Counter-Terrorism Policy: A Critical Assessment' (2015) 30(2-3) Intelligence and National Security 306; Vavoula (n 2); European Council, 'The European Union Counter-Terrorism Strategy' (2005) Doc. No. 1446/4/05 REV 4, <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2014469%202005%20REV%204> accessed 22 September 2020.

[38] Ryszard Cholewinski, 'The Criminalisation of Migration in EU Law and Policy' in Annaliese Baldaccini, Elspeth Guild and Helen Toner (eds), *Whose Freedom, Security and Justice? EU Immigration and Asylum Law and Policy* (Hart Publishing 2007), 306.

[39] Baldaccini (n 1); Humphrey (n 25).

[40] Humphrey (n 25); Valsamis Mitsilegas, 'The Transformation of Privacy in an Era of Pre-Emptive Surveillance' (2015) 20(1) Tilburg Law Review 35.

[41] For detailed discussions on the various ways that this can occur, *see* Gian Luigi Gatta, Valsamis Mitsilegas and Stefano Zirulia (eds), *Controlling Immigration Through Criminal Law: European and Comparative Perspectives on Crimmigration* (Bloomsbury Publishing 2021)and Neža Kogovšek Šalamon (ed), *Causes and Consequences of Migrant Criminalization* (Springer, 2020).

[42] Le'onard (n 37).

terrorism.[43] This move was made easier due to the generalised suspicion with which migrants are subjected to – with no clear notion of who might pose a threat, states instead constructed a risk profile which generated suspicion towards anyone who might be considered as sharing the characteristics of those who had committed acts of terror.[44] Immigrants fell squarely within this risk profile, and consequently managing immigration became classed as an important priority.

This process was accelerated following a surge in terrorist attacks within Europe between 2015-2018. While international terrorism was not a new phenomenon for the EU's thread radar, this surge coincided with an unprecedented increase in the number of asylum seekers attempting to travel to the territory of the EU.[45] Overwhelmed by the sheer numbers of migrants arriving on their shores, several EU states were unable to adequately process migrants on their arrival, allowing them to travel onwards into the territory of Europe undetected. This led to fears that terrorists would attempt to utilise these uncontrolled movements in order to enter the territory of EU undetected – fears which have been validated through cases such as Abdelaziz al H. and his brother Abdelfatah al H, two members of the terrorist group Jabhat al-Nusra who managed to enter the EU by posing as refugees.[46][47]

Therefore, it should be recognised that the task of protecting the borders of Europe is not simple, but rather one which requires a great deal of intricacy and cooperation. After all, authorities need to be able to identify those who are legitimate travellers and facilitate their travel, while at the same time reducing the porosity of the borders in order to decrease the number of irregular border crossings. Simultaneously, these actors also need to identify potential threats and ensure that they are stopped before they enter the territory of the Union. Achieving these aims therefore requires an increasingly diverse group of actors to collaborate with each other.

[43] Perruchoud (n 24); United Nations Counter-Terrorism Centre, *Handbook on Human Rights and Screening in Border Security and Management Pocketbook* (United Nations Office of Counter-Terrorism 2018), available at <https://www.un.org/sites/www.un.org.counterterrorism/files/1806953-en-ctitf-handbookhrscreeningatborders-for-web2.pdf> accessed 16 September 2020.

[44] Didier Bigo, Sergio Carrera, Ben Hayes, Nicholas Hernanz and Julien Jeandesboz, 'Justice and Home Affairs Databases and a Smart Borders System at EU External Borders: Evaluation of Current and Forthcoming Proposals' (2012) 52 *CEPS Paper in Liberty and Security in Europe* 1-91; d'Appollonia (n 14).

[45] Tiekstra (n 16); Hartmut Aden, 'Interoperability Between EU Policing and Migration Databases: Risks for Privacy' (2020) 26(1) European Public Law 93; Vavoula (n 2).

[46] Tiekstra (n 16); Teresa Quintel, 'Connecting Personal Data of Third Country Nationals: Interoperability of EU Databases in the Light of the CJEU's Case Law on Data Retention' (2018) University of Luxembourg Law Working Paper No.002-2018 <https://ssrn.com/abstract=3132506> accessed 8 March 2021.

[47] It should be noted, however, that despite this case, there is little evidence to suggest that the migration crisis has been exploited by terrorists on a widescale basis.

2.2 Conflict with human rights

All these factors have led to a situation where migration is now commonly *'seen through [a] law enforcement lens'*[48] as opposed to being understood purely as an immigration issue. Viewing migration this way can have important implications for human rights. Specifically, this concerns the rights to privacy and data protection, as protected under Article 8 of the European Convention on Human Rights (ECHR)[49] and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (EU Charter).[50]

Many of these new technologies implemented within the border security field rely on the collection and storage of personal information, specifically biometrics, which can have serious privacy implications for an individual. Every year, the amount of information collected only increases. Due to its importance to the national security of a country, a State's border has always been an area in which human rights are entitled to be restricted. States are entitled to demand to know who a person is, why they wish to travel to their country, and mandate that they provide enough evidence to prove the truth behind their answers.

Nevertheless, this does not mean that states are no longer bound by their human rights obligations. Indeed, as the UN Counter-Terrorism Centre has noted, states need to ensure that any measures they chose to use in combating threats that might arise at their border, such as irregular migration or terrorism, do not *'adversely affect the enjoyment of the human rights and dignity of people at the border.'*[51] It should be noted that *'the objectives of combating terrorism or violent extremism do not override a State's international human rights obligations.'*[52]

Therefore, while states have a legitimate interest which permits them to limit the protection of human rights at their border, they are constrained to use this power only where necessary and proportionate to do so. Effective border security is therefore all about finding balance – between protecting human rights, facilitating migration, and safeguarding the security of the state through implementing efficient border control measures which identify and thwart threats before they reach the state's territory.

3. A holistic approach: the ecosystem concept

The question therefore is how can this balance be achieved? How can states balance these competing interests which are inherent to the protection of the state? How can we ensure that the methods utilised do not unnecessarily infringe on the rights of migrants?

[48] Perruchoud (n 24), 135.

[49] Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos.11 and 14 (ECHR) (1950) ETS 5.

[50] Charter of Fundamental Rights of the European Union [2012] OJ C326/02.

[51] United Nations Counter-Terrorism Centre (n 43), 3.

[52] *Ibid* 3.

In this article it is proposed that before an adequate answer to this question can be reached, it must first be accepted that the situation is much more complex and interconnected than it might first appear. Particularly within Europe, the field of border security has come to be recognised as one requiring a significant degree of cooperation and collaboration from an increasingly diverse range of sources. This realisation can be attributed to two main causes: firstly, the rise of international terrorism; and secondly, the refugee crisis. These events have highlighted the importance of states working together with their neighbours, the international community, and industry partners, in order to ensure the effective maintenance of security. Border security has therefore become an ecosystem.[53]

Divested from its original roots within the ecological sciences, the ecosystem concept offers a way through which to understand, study and analyse complex and interconnected groups of actors engaged in the exchange of information and resources, like that which has formed in the field of border security.[54] By understanding that these groups of actors are working together in a system, it becomes possible to appreciate how each individual element or actor can influence those around them and the consequences that this might have for human rights.

Moreover, in looking at the various actors as part of a connected system, it becomes possible to consider the situation from a more holistic perspective and appreciate how cumulative interferences with human rights could lead to a violation of an individual's rights.[55] However, in order to do this, it is first important to understand the three central tenets of the ecosystem concept.

(1) Interconnections

In ecology, the ecosystem concept has played a crucial role in understanding how ecological communities have come to be formed, through focusing on how the various living and non-living organisms interact with each other.[56] An important step is therefore recognising that all the various elements of the ecosystem are interconnected, and it is this interconnection which enables them to share information and resources.

Rather than representing a range of actors pursuing a similar goal, they should be recognised as being *'integral part[s] of a single system.'*[57] Such is the importance of the interconnections between them that it becomes impossible to isolate and analyse each

[53] For a detailed discussion on the ecosystem concept and its applicability as a method for balancing competing human rights, *see* Lauren E. Elrick, 'The Ecosystem Concept: A Holistic Approach to Privacy Protection' (2021) 35(1) International Review of Law, Computers and Technology 24.

[54] Elrick (n53).

[55] *Ibid.*

[56] Arthur G Tansley, 'The Use and Abuse of Vegetational Concepts and Terms' (1935) 16(3) Ecology 284; Froukje Maria Platjouw, *Environmental Law and the Ecosystem Approach: Maintaining Ecological Integrity Through Consistency in Law* (Routledge 2016).

[57] Platjouw (n 56), §1.4.1.

actor independently – indeed, their behaviour is so interconnected that attempting to analyse them separately would only lead to flawed results.[58]

While the precise make-up of the different actors within the ecosystem is an important consideration, it will be the interconnections between them that will determine why the ecosystem works in the way it does.[59] Thus, interconnections are a central element of the ecosystem concept – the ecosystem is considered a system because it works as a whole and not as a collection of individual parts. Consequently, to understand why an ecosystem works as it does, the various actors must be considered together.

(2) Interactions

While it is vital to identify how the different actors within a system are interconnected, it is equally as important to understand how the actions of one might affect others within the system. Due to the close interconnections between them, it is highly likely that the actions of one actor will influence the actions of others within the system.[60] This is because the actors within an ecosystem are engaged in a series of constant interactions – in a biological ecosystem, this is how information and resources are shared.[61]

Due to these constant exchanges, it is possible for certain actors to exert a significant influence over others – potentially at the expense of other actors who will be disproportionately affected as a result.[62] Interactions are therefore important because they explain how the various elements of the system rely on each other, and consequently, help to identify how changes to one element of the system might have wider effects throughout the system.

(3) The non-living element

The third and final element to consider is that of the non-living elements. When devising his initial concept of the ecosystem, Sir Arthur Tansley was motivated by a desire to prompt ecology to pay greater attention to the role played by non-living elements in the development of ecological communities.[63] Writing in 1935, Tansley reasoned that *'our natural human prejudices force us to consider the organisms… as the most important part of these systems, but certainly inorganic 'factors' are also parts – there could be no system without them.'*[64] For Tansley, the role played by these non-living elements of the system had for too long been overlooked, hidden under the shadows cast by the living elements

[58] Platjouw (n 56), §3.1; Tansley (n 56); Elrick (n 53).

[59] Platjouw (n 56); Elrick (n 53).

[60] Platjouw (n 56); JA Russell et al, 'Systems and Ecosystems' in Martin A Abraham (ed), *Sustainability Science and Engineering: Defining Principles* (Elsevier 2006).

[61] Russell et al (n 60); Tansley (n 56).

[62] Elrick (n 53).

[63] Tansley (n 56); Frank B Golley, *A History of the Ecosystem Concept in Ecology: More Than The Sum Of The Parts* (Yale University Press 1993).

[64] Tansley (n 56), 299.

of the ecosystem – they were considered a *'secondary factor,'* elegantly described as *'a stage on which the biota acted a drama.'*[65]

However, by failing to appreciate the role played by these non-living elements, it became impossible to truly understand how an ecosystem operated. Afterall, these non-living elements were interconnected to the living elements – they interacted with them, sharing resources and information between each other. If those studying the system chose to overlook the role played by the non-living elements, they would never truly understand it - for it would be impossible to fully understand the inner workings of the ecosystem without them. The non-living elements were an integral part of the system.

3.1 A border security ecosystem?

The core of the ecosystem concept can therefore be distilled into three elements - interconnections, interactions, and the vital role played by the non-living elements of the system. The question remains, however, as to how this is relevant to the field of border security – how can, or rather why should, border security be thought of as an ecosystem? And how would it benefit immigrants – whether they be refugees, asylum seekers, or economic migrants?

As mentioned, the range of actors involved in the field of border security has dramatically increased over the past few decades.[66] The border has become deterritorialised – expanding outward into neighbouring states and contracting inward to capture even those who not in the border area.[67] The border is no longer a singular line, but rather a fluid zone, constantly moving in order to detect potential threats and prevent them before they occur.

Consequently, by stretching away from their actual geographical locations, borders have become *'instruments of remote control'*[68] causing the previously separated domains of internal and external security to become increasingly intermingled.[69] Additionally, through a process of digitalisation, the border has also become omnipresent, portable, and virtual.[70] As such, it is no longer the case that individuals can be subjected to border controls solely

[65] Golley (n 63), 24.

[66] Julien Jeandesboz, 'Smartening Border Security in the European Union: An Associational Inquiry' (2016) 47(4) Security Dialogue 292.

[67] Ayelet Shachar, *The Shifting Border: Legal Cartographies of Migration and Mobility - Ayelet Shachar in Dialogue* (Manchester University Press 2020); Susana Ferreira, *Human Security and Migration in Europe's Southern Borders* (Palgrave Macmillan 2019); Didier Bigo, 'Security, Borders and the State' in Paul Ganster, Alan Sweedler, James Scott and Wolf Dieter-Eberwein (eds), *Borders and Border Regions in Europe and North America* (San Diego State University 1997).

[68] Huub Dijstelbloem and Dennis Broeders, 'Border Surveillance, Mobility Management and the Shaping of Non-Publics in Europe' (2015) 18(1) European Journal of Social Theory 21, 25.

[69] Bigo (n 67); Didier Bigo, 'Internal and External Aspects of Security' (2006) 15(4) European Security 385.

[70] Dijstelbloem and Broeders (n 68), 25.

at the border itself, but rather they have become part of a much larger process, exemplified through *'monitoring, admission requirements and administrative processes.'*[71]

As the European Commission highlighted in their *European Agenda on Security*:

'in recent years new and complex threats have emerged highlighting the need for further synergies and closer cooperation at all levels… Threats are becoming more varied and more international, as well as increasingly cross-border and cross-sectorial in nature.'[72]

Consequently, this also requires that those actors involved in protecting against these threats become more varied, more international, and, more cross-sectorial. As a result, the actors found within the border security field come from a range of fields (border control; visa, asylum and immigration authorities; customs officials; law enforcement and judicial authorities; vehicle registration authorities; air carriers etc).

Moreover, these actors originate from a variety of different levels including the national (domestic law enforcement authorities, border guards and immigration officials); the regional/European (including EU institutions and agencies such as Europol, Eurojust and the European Border and Coast Guard Agency); and the International (e.g. Interpol and third-country states) and even the private sector (i.e. airline operators).[73]

In order to combat these new complex cross-border threats, what is required is greater cooperation – between agencies, States, and, different sectors. For example, the case of Youssef Zaghba is evidence of what can happen when the necessary cooperation cannot be found. Zaghba was one of the terrorists responsible for the London Bridge attack in 2017. After having been stopped at Bologna Airport, Italian authorities believed that he posed a terrorist threat and decided to place an alert on Zaghba within the SIS.[74]

[71] Dijstelbloem and Broeders (n 68), 25; Matthias Leese, 'Fixing State Vision: Interoperability, Biometrics, and Identity Management in the EU' (2020) Geopolitics, DOI: 10.1080/14650045.2020.1830764.

[72] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, The European Agenda on Security' COM(2015) 185, 2.

[73] Gutheil et al (n 6); Cristina Blasi Casagran, 'Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU' (2021) 21(2) Human Rights Law Review 433.

[74] An alert is defined within Article 3(1)(a) of Council Decision 2007/533/JHA as the set of data that shall be entered into SIS II in order to enable competent authorities to identify a person or object which should be the subject of a specific action. The grounds for issuing a serious crime alert can be found within Article 36(2) of the aforementioned Decision which specifies that an alert for a discreet or specific check can be issued for the purposes of 'prosecuting criminal offences and…the prevention of threats to public security.' Meanwhile, Article 36(3) provides that an alert can also be issued if there is a 'concrete indication' that the alert is 'necessary in order to prevent a serious threat… to internal or external national security.' In this case, the Member State shall inform the other Member States of this increased risk.

However, the Italian authorities listed Zaghba as a serious crime alert, rather than a national security alert.[75] This was an important distinction as while a serious crime alert can relate to a long list of offences,[76] a national security alert is intended to highlight the distinct characteristics of such a threat and differentiate it from other categories of crime.

Consequently, since the wrong category of alert was used, the information about the alert was not passed from the National Crime Agency (the UK's national law enforcement agency dealing with serious crimes) onto MI5 (who deal with domestic counterintelligence and security issues). It is clear from the case of Zaghba that there were a series of failures in the cooperation between the various actors – both internationally and domestically. Accordingly, in order to effectively ensure the protection of a state's internal security, those involved in the attainment of multiple different aims must work together in order to achieve their common goals. Within Europe, this has resulted in the spheres of *'border management, law enforcement and migration control [becoming] dynamically interconnected.'*[77]

This process can be exemplified through the fact that over the years, a range of measures have been developed through which the movement of TCNs has come to be regulated (through the development of large-scale IT databases in the areas of migration and asylum) and securitised (with data primarily been collected for immigration purposes increasingly been used for the achievement of security-related goals). As the ECtHR has acknowledged in Beghal v UK,[78] States face a *'very real threat'*[79] from international terrorism. Consequently, *'controlling the international movement of terrorism'*[80] is highly important.

To facilitate this, *'ports and border controls will inevitably provide a crucial focal point for detecting and preventing the movement of terrorists and/or foiling terrorist attacks.'*[81]Statements such as this have helped to develop a rhetoric through which the movements of TCN have come to be repeatedly linked to the pursuit of security related goals. While this statement by and of itself is not controversial – border controls do have the potential to play an important role in the detection and prevention of international terrorism – the problem relates back to how border controls have been used to control international movement in practice.

The refugee crisis in 2015, combined with the backdrop of recent terrorist attacks, created a *'window of opportunity'*[82] through which the EU has been able to accelerate proposals so

[75] Dominic Grieve, 'The 2017 Attacks: What Needs to Change?' (Intelligence and Security Committee of Parliament 2018) *HC 1694*, para 208.

[76] Which can be found within Art 2(2) of Council Framework Decision 2002/584/JHA. See Art 36(2), Council Decision 2007/533/JHA.

[77] COM(2016) 205 final, 2.

[78] [2019] ECHR 181.

[79] *Ibid* para 92.

[80] *Ibid* para 92.

[81] *Ibid* para 92, *emphasis added.*

[82] Aden (n 45), 98.

as to develop new databases used to monitor TCNs arriving within the territory of the EU.[83] These new systems help to highlight the role of the border as a *'site of identity production'*[84] through which anyone who is not an EU citizen is increasingly required to prove their identity through a series of *'rigid identification and registration procedures.'*[85]

Depending on the individual characteristics of the immigrant (asylum seeker, visa holder, visa-exempt traveller), how they are required to prove their identity varies. This desire to gain a complete picture of TCNs stems from efforts to realise the principle of *'the more you know, the better.'* The more individual data points you have about a person, the more *'unequivocally distinguishable'*[86] they become to state authorities.

Consequently, each time a TCN interacts with the EU border, they are required to provide evidence which can be authoritatively verified as proving their identity. This interaction between the TCN and the respective authority (whether they be border guards, visa authorities or asylum officials) is nothing new. However, a second stage of interactions have begun to occur – where the information provided by the TCN in order to verify and authenticate their identity has also been used for the achievement of security related goals. This trend has become increasingly common and has resulted in the distinct spheres of migration control and internal security becoming increasingly intermingled.[87]

This intermingling has resulted in the field of EU border security becoming progressively complex. Yet, just because an area is complex does not mean that it should necessarily be thought of as an ecosystem. Rather, the definitive reason why border security should be thought of this way can only be seen by taking a closer look at the precise make-up of the field. In particular, it is important to play close attention to not only the number of actors present, but also their composition. What soon becomes clear is that within the border security sphere, there is an entity which is often overlooked but which plays an important role in the functioning of the field. Over the years, those tasked with effectively maintaining the border security field have come to rely upon an increasingly diverse and ever-growing range of technologies which are used to track and monitor individuals as they travel over borders. It is for this reason that border security can be conceptualised as an ecosystem – border security has a *'non-living element.'*

The presence of these technologies within the border sphere has resulted in it being transformed into a *'dense socio-technical environment'*[88] where the range of entities composing it are *'not strictly technical, nor exclusively human.'*[89] Rather, there is a

[83] Aden (n 45); Teresa Quintel, 'Interoperability of EU Databases and Access to Personal Data by National Police Authorities under Article 20 of the Commission Proposals' (2018) 4(4) European Data Protection Law Review 470.

[84] Leese (n 71), 1.

[85] *Ibid* 1.

[86] *Ibid* 4.

[87] Quintel (n 13); Vavoula (n 13).

[88] Rocco Bellanova and Denis Duez, 'A Different View on the 'Making' of European Security: The EU Passenger Name Record System as a Socio-Technical Assemblage' (2012) 17 European Foreign Affairs Review, Special Issue 109, 110; Jeandesboz (n 66).

[89] Jeandesboz (n 66), 292.

combination of both – with the work of the human elements becoming increasingly dependent on the technical. And much like Tansley feared in relation to ecology, there is a tendency to ignore the role played by the non-living elements of the border security sphere and absolve them of responsibility for the consequences they produce.

Therefore, just like ecology believed that the non-living element was inconsequential, so too have we come to treat the technology used within the border security sphere as an insignificant component – as a non-living, neutral element which is not capable of affecting the results of how the system operates. But, as ecology has come to learn, this is not the case. The non-living element has a crucial role to play, influencing the decisions made and having consequences for other actors in the system – in our current case, the migrants attempting to cross a border. As we increase the amount of technology present, we give it a role of larger and larger importance. Accordingly, it is vitally important to understand the consequences of doing so. Technology is not neutral – like the non-living elements of biological ecosystems, technology helps to shape and influence the ecosystem in which it is found.

4. Testing the concept: border security in the European Union

Over the years, the European Union has developed a range of tools in order to facilitate their ability to track, monitor, and, assess individuals as they travel over the borders of the European Union.[90] This information is collected and stored in a series of large-scale information systems and databases which enables authorities to determine whether an individual should be permitted or denied entry to the territory of the EU.

This concept of a border security ecosystem shall therefore be tested by examining how, through developing these databases, the field of border security within the EU has been transformed to such an extent that these non-living elements must now be considered integral parts of the system. There are currently six databases which are of interest: SIS, VIS, Eurodac, EES, ETIAS and the ECRIS-TCN. The final three databases are not yet currently in use but are due to come into operation soon. Each of these databases pursue specific objectives, explained briefly below.

(1) The Schengen Information System (SIS)

The SIS is the largest information system for security and border management in use within the European Union.[91] It was established following the entry into force of the Schengen Convention (1990)[92] in order to compensate for the Schengen Area's lack of internal borders. It enables national authorities to enter alerts, such as that issued for Zaghba, on a

[90] Brouwer (n 13).

[91] European Commission, 'Schengen Information System' (2020) <https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en> accessed 25 September 2020.

[92] Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders [2000] OJ L 239/19.

wide range of issues – such as persons wanted for arrest, missing persons, stolen vehicles, and firearms, as well as TCNs who are to be refused entry to the European Union. These alerts can then be consulted by competent national authorities, such as police or border officials.

(2) The Visa Information System (VIS)

The VIS was created in order to enable the collection and storage of fingerprints and other biometric identifiers from all TCNs applying for a short-term visa. Its creation was justified on the basis that such information was necessary in order to enable authorities to determine whether the individual presenting themselves at the border was who they said they were. It has been acknowledged that the use of the data collected within the VIS can *'contribute towards internal security and combatting terrorism'*[93] and so a legal basis allowing Member State authorities responsible for internal security access to VIS data (where necessary) was established.[94] In this way, it becomes clear how data collected within one field (migration management) becomes relevant for another (internal security and counterterrorism). Discussions are currently ongoing regarding revising the VIS system.[95]

(3) European Asylum Dactyloscopy (Eurodac)

Eurodac was primarily created in order to help facilitate the fair distribution of responsibility for assessing asylum applications, as envisaged under the Dublin Regulation (2013).[96] Consequently, the Eurodac Regulation (2000)[97] established a system for storing the fingerprints of all individuals over the age of 14 who apply for asylum within an EU Member State, allowing Member States to check whether an individual requesting asylum had previously been registered within the system by another Member State. In its original format, Eurodac was therefore an immigration database.

However, the Eurodac Regulation was recast in 2013, in order to enhance its functions and provide access for law enforcement authorities (where necessary to facilitate the prevention, detection and investigation of serious crimes and terrorist offences).[98] The

[93] Council Decision 2008/633/JHA of 23 June 2008 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 L 218/129, preamble.

[94] Council Decision 2008/633/JHA.

[95] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008' (VIS Proposal) COM(2018) 302 final.

[96] Regulation (EU) 604/2013 of 26 June 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 [2013] OJ L 180/31.

[97] Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention [2000] OJ L 316/1.

[98] Regulation (EU) No 603/2013 of 26 June 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

Regulation notes that despite its original purpose, the data contained within the database is useful for those investigating serious crimes and terrorist offences – such as for the comparison of fingerprints found at a crime scene – and consequently, established rules providing access to this information.[99] Under this, we can see how an immigration database has been reformulated to also be a security database and how the category of migrant has been reformulated into a category of risk.

Moreover, following the migration crisis in 2015, there have been calls for Eurodac to be reformed once again. Proposals for reform highlighted that there was now a greater need for Member States, including those not at the external borders, to be able to *'store and compare information on… irregular migrants'*[100] found within their territory, particularly if they had not applied for asylum, as otherwise *'thousands of migrants [would] remain invisible [within] Europe.'*[101] The proposals would require the collection of new categories of personal data, such as name, date of birth, nationality, and, identity documents.[102]

(4) The Entry-Exit System (EES)

The EES will store information on all third-country nationals, including those who are visa exempt. This automated IT system will record whenever a third country national crosses the EU's external border, registering their name, type of travel document, biometric data (such as fingerprints and facial images), as well as the place, and date, of entry, and exit.[103] It will also record whenever an individual is refused access to the EU. The EES is envisaged as being both an immigration and a security database.

Accordingly, the Regulation notes that the objectives of the EES should be to *'improve the management of external borders, to prevent irregular migration and to facilitate the*

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 L 180/1.

[99] Regulation (EU) No 603/2013, preamble.

[100] European 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)' (Eurodac Proposal) COM(2016) 272 final, 2.

[101] *Ibid.*

[102] COM(2016) 272 final, Arts 12-14.

[103] Regulation (EU) 2017/2226 of 30 November 2017 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 L 327/20.

management of migration flows'[104] while additionally contributing to the *'prevention, detection and investigation of terrorist offences and of other serious criminal offences.'*[105]

(5) The European Travel Information and Authorisation System (ETIAS)

The ETIAS is also designed to record data on those non-EU nationals not required to apply for a visa. Rather, they will be required to apply for a travel authorisation prior to their trip. The information collected will be used to assess whether the individual poses a security threat or are likely to engage in irregular migration.[106] After applying, the system will check whether any information on the individual is contained within any of the other European databases – SIS, VIS, EES or Eurodac, as well as against Europol and Interpol databases (such as Interpol Stolen and Lost Travel Documents (SLTD) or the Interpol Travel Documents Associated with Notices (TDAWN) – in addition to the ETIAS system's own watchlist and set of specific risk indicators.[107]

This process should take place automatically, however if the system records a *'hit'* – indicating that the individual has been identified within one of these systems – then the application will have to be processed manually. The ETIAS will require that the individual provide a significant quantity of personal data, listed within Article 17, Reg (EU) 2018/1240. While the ETIAS holds details on migrants, it has specifically been envisaged as a security database, with its purpose being to enable *'consideration of whether the presence of those third-country nationals [who are visa exempt] in the territory of the Member States would pose a security, illegal immigration or high epidemic risk.'*[108]

(6) The European Criminal Records Information System – Third Country Nationals (ECRIS-TCN)

The final database, the ECRIS-TCN, has been specifically designed in order to address a discrepancy between how the criminal records of EU nationals and TCNs are exchanged. ECRIS-TCN will establish a centralised system through which a Member State can identify which other Member States might hold information in relation to any convictions of a TCN.[109] Whenever a third country national is convicted of a crime (as well as those who have previously been convicted), the convicting Member State shall be required to create a data record in the ECRIS-TCN central system.[110] This data record shall contain both alphanumeric data (such as full name and date of birth) and biometric data (such as

[104] Regulation (EU) 2017/2226, preamble

[105] *Ibid.*

[106] Regulation (EU) 2018/1240 of 12 September 2018 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 L 236/1.

[107] *Ibid*.

[108] *Ibid* Art 1.

[109] Regulation (EU) 2019/816 of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 [2019] OJ L 135/1.

[110] *Ibid* Arts 1 and 5.

fingerprints, where legally entitled to be collected, or facial images).[111] In this case, while the ECRIS-TCN was created for security reasons, it is composed solely of immigrants.

From a brief examination of these databases, it becomes clear how the issues of immigration and security have become bound together and how this has been facilitated through the use of technology. This shows how the movements of TCNs have increasingly come to be regulated, in order to assess whether they pose a security risk.[112] Nonetheless, as they currently are, these systems are separated; the information within them is confined to their own distinct spheres. However, in 2019 two Regulations were adopted in order to enable interoperability between the different systems.[113] It is through this interoperability that we can see how the various spheres of information have become bound more tightly together, forming an ecosystem of information.

4.1 'A complex landscape': a network of databases

With such a diverse range of databases, each of which contains its own spectrum of information, there has long been discussions as to how to use this information more effectively. One method which has repeatedly been suggested is to enhance interoperability between the different systems. Interoperability refers to *'the ability of different information systems to communicate, exchange data and use the information which has been exchanged.'*[114]

The EU considers that it should be thought of as a *'technical rather than a legal or political concept.'*[115] However, the EDPS thinks differently and, in his view, the concept *'cannot be disconnected from the questions [of] whether the data exchange is necessary, politically desirable or legally possible.'*[116] From a technical perspective, interoperability can be understood as representing a method through which these various large-scale databases can be linked together, to make the sharing of information between them easier.[117] Without the delays caused by the currently fragmented data management system, national authorities and EU bodies would be able to search and access the information contained within these systems more efficiently (provided they are entitled to access the data).[118]

[111] *Ibid* Art 5.
[112] Vavoula (n 2).
[113] Reg (EU) 2019/817; Reg (EU) 2019/818.
[114] EDPS, 'Reflection Paper on the Interoperability of Information Systems in the Area of Freedom, Security and Justice' (2017), para 7 <https://edps.europa.eu/sites/edp/files/publication/17-11-16_opinion_interoperability_en.pdf> accessed 30 September 2020/9/2020.
[115] European 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, 3.
[116] EDPS (n 112), para 7.
[117] Deirdre Curtin and Filipe Brito Bastos, 'Interoperable Information Sharing and the Five Novel Frontiers of EU Governance: A Special Issue' (2020) 26(1) European Public Law 59; Brouwer (n 13).
[118] COM(2016) 205 final, 3-4; Brouwer (n 13).

The European Commission clearly sets out their justification for the necessity of interoperability within the Communication, '*Stronger and Smarter Information Systems for Borders and Security.*'[119] This acknowledges that, despite there being a number of IT systems and databases which can be accessed by border guards, police officials and other national authorities in the course of their duties, there are shortcomings related to these systems which *'impede the work of these national authorities.'*[120] These shortcomings directly relate to the fact that:

'[The EU's current] architecture of data management for border control and security is marked by fragmentation… caused by the various institutional, legal and policy contexts in which the systems have been developed. Information is stored separately in various systems that are rarely interconnected. There is inconsistency between databases and diverging access to data for relevant authorities. This can lead to blind spots notably for law enforcement authorities.'[121]

One of the fears of the Commission was that due to this fragmentation of information across the various databases, there would be a possibility that information would fall through the cracks and not reach the agencies which required it.[122] The resulting consequence would be that, like in the case of Zaghba, the appropriate authorities would not be aware of the security threat until it was too late to prevent it.[123]

In order to rectify these issues, Regulations (EU) 2019/817 and 2019/818 were adopted. Together, they are designed to implement a system of interoperability between EU information systems in the fields of borders and visas; and police and judicial cooperation, asylum and migration respectively. In order to pursue several objectives,[124] these twin regulations establish four different components recognised as necessary in order to achieve interoperability between the information systems: firstly, a European Search Portal

[119] COM(2016) 205 final.

[120] *Ibid* 3-4.

[121] *Ibid* 3-4.

[122] Aden (n 45).

[123] The qualifier, of course, is that interoperability would still not have prevented the problem which resulted in the Zaghba case from occurring. In this specific case, the failure was down to the incorrect qualification of the alert – a human failure – rather than the inability of the systems to connect information.

[124] These objectives include: (a) improving the effectiveness and efficiency of border checks, (b) combatting and preventing illegal immigration, (c) enhancing the overall security of the Area of Freedom, Security and Justice, (d) improving the implementation of the common visa policy, (e) assisting in the examination of applications for international protection, (f) preventing, detecting and investigating terrorist offences and (f) facilitating the identification of unknown persons unable to identify themselves - Art 2(1), Reg (EU) 2019/817 and Art 2(1), Reg (EU) 2019/818. The Regulations seek to achieve these objectives though (a) ensuring the correct identification of individuals, (b) combating identity fraud, (c) improving data quality and harmonising data storage requirements between EU information systems, (d) facilitating and supporting the operational implementation of the individual systems by Member States, (e) strengthening, simplifying and enhancing uniformity in the data security and data protection conditions of the respective EU information systems, (f) streamlining access conditions for designated authorities and (g) supporting the purposes of the SIS, VIS, Eurodac, EES, ETIAS and ECRIS-TCN – Art 2(2), Reg (EU) 2019/817 and Art 2(2), Reg (EU) 2019/818.

(ESP); secondly, a shared Biometric Matching Service (BMS); thirdly, a Common Identity Repository (CIR); and fourthly, a Multiple-Identity Detector (MID).[125]

The first component, the ESP, will enable users to simultaneously query multiple systems (the six databases, in addition to Europol and Interpol databases) at one time using an individual's identity data (either biographical or biometric).[126] The system will then return a result indicating to the user whether any information is contained within any of the systems to which they have access.[127] The BMS enables the user to query and compare biometric data (fingerprints and facial images) contained within any of the central systems (specifically, SIS, VIS, Eurodac, EES and ECRIS-TCN).[128]

Consequently, rather than having to use the individual search engine for each system, the BMS would enable the user to do one single search. The CIR will provide a shared central storage point for the biographical and biometric data of TCNs that is currently recorded (or will be recorded) in Eurodac, VIS, EES, ETIAS and ECRIS-TCN.[129] Thus, while several systems might hold information on the same individual, within the CIR each individual will only have one file which links to all of the data held in the respective systems.[130] Utilising a hit/no hit system, it will be possible to determine whether any of the systems hold information on a specific individual.

Finally, the MID will examine the various databases in order to determine whether the identity data on which the search has been conducted is present in more than one of the information systems.[131] The search will look to determine whether more than one identity has been linked to the same set of biometric identifiers. If these identifiers are found within more than one system, then the link will be categorised with a specific colour: (i) yellow (potential differing biographic identities); (ii) white (different biographical identities link to the same *bona fide* individual); (iii) green (different *bona fide* persons sharing the same biographic identity); or (iv) red (suspicions exist that one individual is unlawfully using multiple biographical identities). These colour-coded links will indicate whether additional attention is required.[132] Together, these four components are intended to ensure that the central objectives of interoperability as indicated within Article 1 of the Regulations are achieved.

However, questions have been raised as to the compatibility of these interoperability provisions with several human rights, including but not limited to, the rights to privacy, data protection, and non-discrimination. As has been highlighted, these databases collect a massive amount of personal data, including biometric data, relating to TCNs. While the Interoperability Regulations present these new tools as essential to protecting the borders of Europe and maintaining internal security, they also have implications for human rights

[125] Art 1, Reg (EU) 2019/817; Art 1, Reg (EU) 2019/818.
[126] Art 6, Reg (EU) 2019/817; Art 6, Reg (EU) 2019/818.
[127] COM(2017) 793 final, 6; COM(2017) 794 final, 6.
[128] Art 12, Reg (EU) 2019/817; Art 12, Reg (EU) 2019/818.
[129] Art 17, Reg (EU) 2019/817; Art 17, Reg (EU) 2019/818.
[130] COM(2017) 793 final, 7; COM(2017) 794 final, 7.
[131] Art 25, Reg (EU) 2019/817; Art 25, Reg (EU) 2019/818.
[132] COM(2017) 793 final, 7; COM(2017) 794 final, 7.

which must be considered. It is important to recognise that despite the importance of the goal of preventing terrorism, there are still limits to the measures which it can justify.

Therefore, the achievement of these objectives must be balanced against the protection of human rights. As will be emphasised, a particularly problematic factor is the enhanced ability that these provisions create for law enforcement authorities to access data primarily collected for migration purposes.[133]

5. Finding the Balance

The question, however, is how can this balance be found? One potential answer could be found by returning to the concept of the ecosystem for guidance. If we accept that the field of EU border security bears many of the features of an ecosystem, then it is also possible that this concept could guide us in determining how to balance these two objectives. How might this be achieved?

One method previously proposed is through relying on the concept in order to develop a more holistic approach to assessing the proportionality of infringements to non- absolute human rights, such as privacy and data protection.[134] This approach recognises that in the modern era, an individual's personal data is subjected to an ever-increasing range of infringements from a variety of sources.

However, proportionality assessments as they are currently conducted only focus on a single measure – assessing whether it represents a justifiable intrusion into an individual's rights – as opposed to considering the consequence of that measure within a wider system of privacy infringements.[135] Consequently, while each individual interference might, by itself, represent a proportionate measure, when added together cumulatively this might not be the case. As has been acknowledged, this *'absence of meaningful standards against the cumulative effect of intrusions into the right to privacy should be regarded as a grave threat to the fundamental rights of the individual.'*[136]

The European Commission uses the phrase *'a complex landscape'*[137] to describe the situation faced by state authorities relying on the operation of these large-scale databases in the course of their work. While developed for a range of purposes and objectives, the one feature these databases all have in common is the collection of vast swathes of personal data. Thus, by their very nature, these databases have a considerable negative effect on an individual's enjoyment of their rights to privacy and data protection, as well as other rights such as the right to non-discrimination.

[133] Le'onard (n 37).

[134] Elrick (n 53).

[135] Carolin Kaiser, 'Privacy and Identity Issues in Financial Transactions: The Proportionality of the European Anti-Money Laundering Legislation' (PhD thesis, University of Groningen 2018).

[136] *Ibid* 555.

[137] COM(2016) 205 final, 3.

This is a factor which has been recognised by the Article 29 Working Party who emphasises that because of this, it is:

‘particularly important to take a holistic viewpoint when assessing the interference with privacy and data protection of a new legislative proposal. In order to say whether a new legislative proposal is still proportionate, it is necessary to assess how the new measure would add to the existing ones and whether all of them taken together would still proportionately limit the fundamental rights of data protection and privacy.’[138]

In order to consider the situation holistically, however, you require a method to do this. This can be provided through the ecosystem concept. The ecosystem inherently provides an adept way of identifying the various actors present within any given situation and ascertaining how they are interconnected and interact with one another. Under this, it becomes possible to understand the effect that one particular action might have on the other actors in the system. By applying this method to any new measure intended to restrict the right to privacy, it becomes possible to weigh the various factors against each other and consider what the potential consequences for an individual’s privacy might be.

Consequently, by utilising the ecosystem concept in this manner – as a method through which to analyse a situation holistically – it enables you to consider new measures, such as the Interoperability Regulations, alongside existing measures. This requires you to look at the legislation not in isolation, but rather to examine it within the wider context in which it has developed. Important questions can therefore be asked, such as what do these new measures add to the pursuit of security? How do the new powers created compare to those already in existence? Do these new measures have any unexpected consequences which might negatively affect individuals? Do they effect the delicate balance which exists between ensuring the protection of human rights and achieving security-related goals? What effects will these new powers have on the right to privacy and other human rights? Are the losses to an individual’s privacy greater or less than the gains for security officials?

In answering these, one could begin to consider whether these powers can be justified as necessary and proportionate.

5.1 What new measures do these Regulations create?

The first thing to consider is what do these measures add? The main intention behind the Interoperability Regulations is to create a framework which will allow for greater cross-linking of the data being stored within the various migration and security databases. As the EDPS has acknowledged, interoperability can therefore represent a *‘useful tool to address the legitimate needs of competent authorities using EU large scale information systems’*[139]

[138] Article 29 Data Protection Working Party, ‘Opinion 01/2014 on the Application of Necessity and Proportionality Concepts and Data Protection Within The Law Enforcement Sector’ (2014) 536/14/EN WP 211, 21 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf> accessed 29 September 2020.

[139] EDPS (n 112), para 37.

such as swifter and more streamlined information sharing but only when *'implemented in a well thought-out manner and in compliance with [the] core requirements of necessity and proportionality.'*[140] For example, being able to search all the databases simultaneously through the ESP would significantly reduce the amount of time needed for a search to be conducted.

However, this would only be acceptable if it ensured that the pre-existing conditions for access continue to be respected, by ensuring that only those authorised to do so will be able to access the data stored within the respective systems. The use of interoperability could even benefit data protection in some ways, for instance, by avoiding duplication of data across various databases.[141]

The European Commission has been keen to stress that the interoperability framework is not designed to create new powers and access rights for authorities, but rather simply facilitate the smoother access and exchange of data.[142] Authorities which previously did not have access to certain categories of data shall still be unable to access them, while those who had to fulfil specific criteria in order to gain access will still have to do so.[143] Yet, this point has been contested and will be addressed in more detail below.

5.2 How do these new powers compare with those already in existence?

As the Article 29 Working Party highlighted, any new measure must be assessed alongside those measures already in existence. In this case, this would be the three systems already in operation (SIS, VIS, Eurodac) as well as those currently under development (EES, ETIAS, ECRIS-TCN). In order to determine whether the addition of the new Interoperability Regulations can be considered necessary and proportionate, it is important to first consider whether the underlying databases themselves can be considered as such. The answer to this question could have significant implications for the introduction of interoperability. Afterall, if the underlying databases cannot be considered proportionate, then how can any measures seeking to interlink them?

The necessity and proportionality of the previously mentioned databases should not automatically be assumed. Several authors have raised concerns that they, in fact, cannot be regarded as necessary or proportionate.[144] Eurodac has faced significant criticisms regarding whether it is appropriate for achieving its stated purposes.[145] Others, such as the

[140] *Ibid* para 37.

[141] *Ibid* para 9.

[142] COM(2017) 793 final; COM(2017) 794 final.

[143] COM(2017) 793 final; COM(2017) 794 final; European Union Agency for Fundamental Rights, 'Opinion 1/2018 - Interoperability and Fundamental Rights Implications: Opinion of the European Union Agency for Fundamental Rights' (2018) <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-opinion-01-2018-interoperability_en.pdf> accessed 19 May 2021.

[144] Vavoula, ETIAS (n 16); Vavoula, Consultation of EU Immigration Databases (n 16); Vavoula (n13); Vavoula (n2); Jones (n 16); Tiekstra (n 16); Brouwer (n 13).

[145] Casagran (n 73).

VIS and ETIAS, have been criticised for storing a disproportionate quantity of personal data, the necessity of which can sometimes be questioned.[146] VIS, for example, stores information on visa sponsors,[147] whereas ETIAS mandates knowing an individual's education level.[148] It seems appropriate to note that the introduction of the ETIAS system has previously been rejected due to the fact that *'the potential contribution to enhancing the security of the Member States would [not] justify the collection of personal data at such a scale.'*[149] Additionally, the grounds within the ETIAS system which can be used to justify refusal of entry are incredibly broad and capable of capturing a large number of potential situations.[150] This raises significant proportionality concerns.

The ETIAS has also been criticised for the fact that in order to achieve its aim of identifying previously unidentified TCNs who might pose a future threat, it enables the creation of a platform through which personal data can be subjected to data mining and profiling.[151] As the EDPS has identified, whenever individuals are subjected to computerised decision making, such as profiling, it raises serious *'technical, legal and ethical questions.'*[152] In particular, he notes that profiling is *'indispensably related'* to high degrees of generalisation, uncertainty regarding the correctness of predicted behaviours, and questions regarding the accuracy of the correlations made between detected patterns and the features of individuals.[153]

Consequently, profiling subjects individuals to the risk of being flagged not as a result of their actual actions, but rather because of something they might do in the future – based on specific characteristics they hold, rather than due to individualised suspicions.[154] Such thinking is highly problematic. The SIS has also faced criticisms as a result of its mixed nature as both a security and immigration database. Due to this feature, it holds data on

[146] Niovi Vavoula, 'The 'Puzzle' of EU-Large Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Personal Data Protection' (2019) European Law Review (forthcoming), available at <https://ssrn.com/abstract=3466766> accessed 8 March 2021.

[147] Art 9(4)(f), Regulation (EC) No 767/2008 of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) [2008] OJ L 218/60.

[148] Art 17(2)(h), Regulation (EU) 2018/1240 of 12 September 2018 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 L 236/1.

[149] European Commission, 'Communication from the Commission to the European Parliament and the Council, Smart Borders – Options and the Way Ahead' COM(2011) 680 final, 7.

[150] Tiekstra (n 16).

[151] Vavoula (n 13); Tiekstra (n 16).

[152] EDPS, 'Opinion 3/2017 on the Proposal for a European Travel Information and Authorisation System (ETIAS)' (2017), para 29 <https://edps.europa.eu/sites/default/files/publication/17-03-070_etias_opinion_en.pdf> accessed 8 March 2021.

[153] *Ibid*.

[154] Vavoula (n 13).

both those recognised as posing a security threat, and those who have contravened immigration law.[155]

Since its introduction, the vast majority of alerts entered into the SIS have related to TCNs who should be refused entry to the EU – in 2018, of the 935,497 alerts listed on persons within the SIS, 504,590 related to TCNs who should be refused entry.[156] However, widescale irregularities in how this power is applied has resulted in it being classed as discriminatory, with it being acknowledged that some Member States are significantly more likely to enter an alert than others.[157] Such discrepancies are particularly problematic considering the consequences of having an SIS alert issued against you can include being refused entry to the territory of the EU in the future.

The sheer quantity of individuals whose data shall be captured within the EES has also resulted in questions regarding its proportionality, particularly due to the fact that significant overlaps exist between the data it will collect and that stored within the VIS.[158] Therefore, the added value of this new database has not been clearly established.[159] Claims that it will address the issue of overstayers has also been questioned.[160]

Finally, while the ECRIS-TCN is presented as a measure through which to ensure that the criminal records of TCNs can be exchanged in a manner equivalent to that which exists for EU nationals, it must be recognised that the ECRIS-TCN does not simply represent an extension of the existing ECRIS system. Rather, while ECRIS is a decentralised system, ECRIS-TCN is centralised and provides for the storage and exchange of biometric data, such as fingerprints and facial images.[161]

In contrast, ECRIS does not include biometric data. This has led to allegations that the system is disproportionate, particularly considering that the Commission's own Impact Assessment suggested that a decentralised system would fulfil the specific objectives of the proposal while also better complying with the principle of non-discrimination.[162] Due to these issues, significant concerns can be raised as to the proportionality of interlinking these already fundamentally flawed systems.

[155] Valsamis Mitsilegas and Niovi Vavoula, 'The Normalisation of Surveillance of Movement in an Era of Reinforcing Privacy Standards' in Philippe Bourbeau (ed), *Handbook on Migration and Security* (Edward Elgar Publishing 2017).

[156] Brouwer (n 13), 73.

[157] Mitsilegas and Vavoula (n 154); Vavoula (n 2).

[158] Mitsilegas and Vavoula (n 154).

[159] *Ibid.*

[160] *Ibid.*

[161] Tiekstra (n 16).

[162] European Commission, 'Impact Assessment accompanying the proposal for a Directive of the European Parliament and of the Council 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' SWD(2016) 4 final; Jones (n 16).

5.3 Do they affect the delicate balance which exists between ensuring the protection of human rights and achieving security-related goals?

The next question which must be addressed is whether, and in what way, these measures might affect the balance which must be found between protecting human rights and achieving security-related goals? Like an ecosystem, these databases are *'multi-purpose, dynamic and flexible in nature.'*[163] This can be clearly evidenced through the way in which the purposes behind these databases have been gradually, but consistently, extended – a process highlighting how the lines separating data collected for migration purposes and data collected for security purposes have become increasingly blurred.[164] This section therefore shows the problematic nature of the Interoperability Regulations, which continue this pre-existing trend of facilitating greater and greater access to immigration data for security purposes.

The beginning of this process can be traced back to the SIS. While the SIS, due to its uniquely mixed nature as both a security and migration database has always envisaged and granted law enforcement access,[165] this is not the case for the other databases. Consequently, while the primary purpose of the VIS is to facilitate the implementation of the common visa policy, it only lists the prevention of internal security threats as one of its ancillary purposes.[166]

As a result, by and large, VIS data cannot be accessed for security purposes, unless the specific conditions laid down within Art 3 of this Regulation, and Council Decision 2008/633/JHA are complied with. Even this limited access has been criticised, with authors emphasising that it shows how in the post 9/11 era, immigration data has increasingly come to be seen for its security benefits.[167] At its core, the VIS is designed to facilitate the achievement of the common visa policy. By including security related goals within its remit, visa applicants are unfairly subjected to the processing of their personal data by law enforcement officials.[168]

Eurodac, on the other hand, was originally envisaged purely as an immigration database. However, the law enforcement benefits of the data it contained was quickly recognised, and in 2013 when the Eurodac Regulation was recast, the ability to access Eurodac data for

[163] Niovi Vavoula, 'Interoperability of European Centralised Databases: Another Nail in the Coffin of Third-Country Nationals' Privacy?' (EU Migration Blog, 8 July 2019), available at <http://eumigrationlawblog.eu/interoperability-of-european-centralised-databases-another-nail-in-the-coffin-of-third-country-nationals-privacy/> accessed 8 March 2021.

[164] EDPS, 'Opinion 4/2018 on the Proposals for Two Regulations Establishing a Framework for Interoperability Between EU Large-Scale Information Systems' (2018) <https://edps.europa.eu/sites/edp/files/publication/2018-04-16_interoperability_opinion_en.pdf> accessed 28 September 2020; EDPS (n 112); Tiekstra (n 16).

[165] Mitsilegas and Vavoula (n 154).

[166] Art 2(g), Regulation (EC) No 767/2008; C-492/08 United Kingdom v Council [2010] ECLI:EU:C:2010:631

[167] Mitsilegas and Vavoula (n 154).

[168] *Ibid.*

security purposes was added.[169] As Vavoula and Mitsilegas have recognised, this can be considered particularly problematic considering the sensitive data Eurodac contains.[170]

The development of the three new databases has meant that this connection between using immigration data for security purposes has become even more clear cut. The EES, which like the SIS has also been envisaged as a multi-purpose tool, will grant law enforcement access to its data from the very beginning of its operation.[171] The ETIAS meanwhile directly links the issues of immigration control and security, by listing its primary objective as *'providing for a thorough risk assessment of applicants [i.e. visa-exempt TCNs], prior to their arrival at the external border crossing points'*[172] in order to determine whether they pose a security risk to the territory of the Union.

Through the introduction of the interoperability provisions, this blurring between purposes becomes even more apparent. In particular, replacing the current *'cascade'* search process (which requires an individual search of each database) with the two step *'hit/no hit'* search function enables the strict access restrictions for law enforcement to VIS, Eurodac, EES and ETIAS data to be avoided.[173] These strict conditions for access are designed to respect the primary purposes of the databases (i.e. immigration) and ensure that the pursuit of security goals should largely be regarded as ancillary.[174] Consequently, law enforcement access is *'subject to a series of limitations, tailor-made to the specificities of each database'*[175] and reserved solely for cases which involve *'the prevention, detection or investigation of terrorist offences and other serious crimes.'*[176]

However, through this *'hit/no hit'* process, law enforcement officials are granted access to personal data despite these access requirements. This is because while the current access conditions remain, the *'hit/no hit'* result in and of itself can also reveal information regarding the individual. For example, by indicating that their details are stored within the VIS or Eurodac, it allows interferences to be made regarding their personal life – such as the fact that they are an asylum seeker or are required to have a visa. Likewise, the lack of a *'hit'* indicates that they do not fall within either of these categories – likely meaning that they are an EU citizen and their data could be contained within national databases.

Article 20 of the Interoperability Regulations is also particularly problematic, highlighting one way through which the Regulations have been used in order to create new powers for security purposes. This article provides that police authorities are permitted to carry out checks of the CIR in order to determine the identity of a person. This is limited to specific situations, such as when the police authority is unable to identify a person due to a lack of

[169] Regulation (EU) No 603/2013.

[170] Mitsilegas and Vavoula (n 154), 240.

[171] Mitsilegas and Vavoula (n 154).

[172] Art 4, Regulation (EU) 2018/1240.

[173] Vavoula (n 13); Quintel (n 82); Quintel (n 46); Tiekstra (n 16).

[174] Vavoula, Consultation of EU Immigration Databases (n 16); Quintel (n 46).

[175] Vavoula, Consultation of EU Immigration Databases (n 16), 147.

[176] *Ibid* 147.

identity document,[177] when doubts arise as to the authenticity and accuracy of the document or identity,[178] or, where the individual is unwilling to cooperate.[179]

If a match is found then the CIR allows the official to access the data stored.[180] As Quintel notes, the CIR allows law enforcement access to immigration data for non-law enforcement purposes, potentially exposing individuals to the arbitrary processing of their data.[181] While immigration related identity checks are regulated through the GDPR, linking these CIR searches to law enforcement purposes enables them to be conducted under the Law Enforcement Directive which has much less stringent requirements for processing special categories of data.[182]

Therefore, while there are no doubt credible reasons why law enforcement authorities might wish to access immigration data, it is important not to ignore why and how each individual database came to be created. Each system within the EU's border security field has developed in order to pursue a specific objective - a factor reflected within the architecture of each individual information system and the safeguards which accompany it.[183] While they all process a range of personal data, what is relevant to one system is not necessarily relevant to another – what is collected and stored is influenced by the objectives of the specific system. Tangentially, those actors which are granted access to the information held within a system are specifically chosen – not every actor will be entitled to access every system. These issues have been used to justify the argument in favour of interoperability,[184] but can also be used to question its pursuit. The precise access rights for each system have been deliberately carved out in order to recognise the specific requirements of the relevant actors in their spheres of work. As the EDPS has highlighted, interoperability has the potential to *'permanently and profoundly affect [the] structure and… way of working' of these large-scale databases.'*[185]

Alarmingly, the fact that this use of immigration data for security purposes makes it very difficult to ascertain the relevant data protection provisions which apply when data is processed by authorities who have roles within both the immigration and security fields,

[177] Art 20(1)(a), Reg (EU) 2019/817; Art 20(1)(a), Reg (EU) 2019/818

[178] Art 20(1)(b)-(d), Reg (EU) 2019/817; Art 20(1)(b)-(d), Reg (EU) 2019/818.

[179] Art 20(1)(e), Reg (EU) 2019/817; Art 20(1)(e), Reg (EU) 2019/818.

[180] This right is established within Article 20(3), Reg (EU) 2019/817 and Art 20(3), Reg (EU) 2019/818. Art 18 of these Regulations defines what data is stored by the CIR, and therefore what the official is entitled to access - namely that found in Article 16(1)(a)-(d), Article 17(1)(a)-(c) and Article 18(1) and (2) of Reg (EU) 2017/2226; Article 9(4)(a)-(c), (5) and (6) of Reg (EC) 767/2008 and Article 17(2)(a)-(e) of Reg (EU) 2018/1240.

[181] Quintel (n 82), 472.

[182] *Ibid* 482.

[183] European Union Agency for Fundamental Rights, 'Fundamental Rights and the Interoperability of EU Information Systems: Borders and Security' (FRA 2017) <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-interoperability-eu-information-systems_en-1.pdf> accessed 21 May 2021.

[184] COM(2005) 597 final, 4.

[185] EDPS (n 163), para 25.

such as Europol.[186] Quintel gives the example of a police officer who, while checking data for immigration purposes, discovers links to that individual within a law enforcement database.[187]

In such a situation, it becomes unclear which legal provisions should apply – Regulation (EU) 2016/679 (GDPR)[188] which prescribes strict limits on the use of personal data or Directive (EU) 2016/680 (Law Enforcement Directive)[189] which permits a lower standard for processing when done for law enforcement purposes.

The check was conducted for immigration purposes, the actor conducting it holds a law enforcement role and the data is within a law enforcement database. In such a situation, it is likely that the police officer is not going to ignore the existence of a law enforcement link – however, this blurring of purposes leads to a situation where data protection standards are likely to become weakened and immigration procedures are increasingly going to be utilised opportunistically in order to identify security threats.[190]

5.4 Do these new measures have any unexpected consequences which might negatively affect individuals?

The next issue to consider is what consequences these measures might have for individuals beyond those which are presented by the Commission. Consequently, it must be recognised that while presented as a purely technical measure designed to enable information sharing between the various large-scale databases, the interoperability provisions go significantly further than this, even going so far as to establish both new databases and new processing purposes.[191] This relates to the development of three of the new interoperability components: the CIR, the BMS and the MID. Through the development of these components, data which previously had been stored separately within each of the systems will now be able to be accessed together from one central system.[192]

Despite being termed *'repositories'* or *'components,'* this should not detract from the fact that what these have created are new databases.[193] As Vavoula notes, this is particularly

[186] Quintel (n 13).

[187] *Ibid* 225.

[188] Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[189] Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Framework Decision 2008/977/JHA (Law Enforcement Directive) [2016] OJ L 119/89.

[190] Quintel (n 46).

[191] Casagran (n 73); Vavoula (n 162).

[192] Quintel (n 13).

[193] Vavoula (n 162); EDPS (n 163); Brouwer (n 13).

problematic as through combining information from different systems, authorities will be able to *'draw more precise conclusions on the private lives of individuals'*[194] while also ensuring that data subjects will be unable to foresee how the information they have provided might be used. These new databases also have the effect of creating new processing purposes,. This is particularly problematic since they are not covered by existing legal bases and also provide information to authorities who would not normally be able to access such data under the existing siloed system.[195]

The creation of new databases is particularly problematic when you consider that nearly all (the exception being ETIAS) of these databases routinely store at least some form of biometric information. Leese provides as explanation for this, highlighting that '*by tying identity to the body, biometrics are supposed to produce a form of truth.'*[196] This truth is found through relying on the physical characteristics of the body (such as fingerprints, DNA, bone structure, irises and gait), all features which are unique to an individual and which consequently allows them to be identified to a high degree of certainty.[197]

The ability to uniquely identify an individual means that biometrics are generally considered as representing a particularly intrusive form of personal data.[198] Consequently, it is regulated as special category of personal data within Article 9 of the GDPR.[199] The processing of biometric data is therefore generally prohibited and only permitted in limited cases under strict safeguards.[200] As the ECtHR has established, retaining the biometrics of individuals who are not suspected of committing an offence is likely to lead to stigmatisation and may undermine the presumption of innocence.[201] While in the case of S and Marper, the interference was found to be justified, questions can be raised as to whether this is also the case with the interoperability provisions.

For instance, the case of Schwarz v Stadt Bochum [2013] raised two important points relating to the storage of biometric data, specifically fingerprints. Firstly, the Court highlighted that the interference was proportionate because the fingerprints were not stored centrally but rather remained within the passport which was retained by the individual.[202] Secondly, they considered that while used as a method of ascertaining identity, should a mismatch occur between the stored fingerprints and those provided in person, the individual would not automatically be refused entry to the EU but rather would be required to submit to additional checks in order to confirm their identity.[203]

[194] Vavoula (n 162).

[195] Quintel (n 46), 17; Brouwer (n 13).

[196] Leese (n 71), 7.

[197] Dijstelbloem and Broeders (n 68); Quintel (n 46); Quintel (n 13); Vavoula (n 13); Leese (n 71); Aden (n 45).

[198] C-291/12 Schwarz v Stadt Bochum [2013] ECLI:EU:C:2013:670, para 27

[199] Art 9, Regulation (EU) 2016/679.

[200] Art 9(2), Regulation (EU) 2016/679; Art 10, Directive (EU) 2016/680.

[201] S and Marper v UK [2008] ECHR 178, para 122.

[202] Schwarz v Stadt Bochum (n 198), para 60.

[203] *Ibid* para 44.

Regarding the first point, unlike in the Schwarz case, the Interoperability Regulations will enable the central storage of fingerprints, alongside other forms of biometric data, within the CIR, BMS and MID.[204] The individual has no control over what happens to this data – they do not know how often it is accessed, by who or for what purposes. This makes it difficult for the individual to know whether they have been subjected to an unjustified interference with their rights. Secondly, while Schwarz only envisaged that a mismatch between fingerprints would result in additional checks, it is not unconceivable that more severe results could occur as a result of a mismatch within the interoperability provisions.[205]

For example, if your fingerprints were incorrectly matched with someone who has already been registered within Eurodac then this could result in international protection being refused, or potentially lead to a creation of a red link within the MID, which could result in a refusal of entry. The sheer number of individuals who will be included within the databases also greatly increases the chance of an incorrect hit being produced, particular where there are underlying issues with the quality of the data – as there is with the existing databases, specifically SIS and VIS.[206] Additionally, since biometrics are often considered as representing the *bona fide* truth, how are you supposed to fight back when errors in the matching of biometric data say that you are not who you say you are?

In the same way, the BMS allows biometric data which has been collected for one purpose to be utilised for another. Take, for example, the case of Eurodac. The data provided in this system has specifically been provided by an individual in order to seek asylum within a Member State of the European Union. They have not consented to, nor could they have envisaged, that the personal data they have provided would then be used in order to detect identity fraud.[207] Using data for purposes for which it has not been collected is particularly problematic since it makes data processing less transparent, and generally, the ways in which this information is used – e.g. refusal of entry decisions or visa application backgrounds checks – are already largely opaque to individuals.[208] The BMS also represents a new processing operation, since it generates biometric templates which are then stored within the system.[209] Despite such an opinion being refuted by the European Commission,[210] biometric templates are generally considered to be personal data, since re-identification remains possible in some cases.[211]

In this way, we can see how the Interoperability Regulations have expanded the border security ecosystem, by interconnecting the various databases to create new ones and establish new processing purposes.

[204] Vavoula (n 13).
[205] Brouwer (n 13).
[206] Vavoula (n 13); Quintel (n 13).
[207] Vavoula (n 13).
[208] Aden (n 45), 106.
[209] Quintel (n 46).
[210] COM(2017) 794 final, 7.
[211] Quintel (n 46), 15.

5.5 How do these Regulations affect the rights to privacy and data protection?

The rights to privacy and data protection are protected within Article 8 of the ECHR and Articles 7 and 8 of the EU Charter. Neither of these rights can be recognised as constituting an absolute right, and therefore can be limited for justified reasons, provided for under the terms of Article 8(2) of the ECHR and Article 52(1) of the EU Charter. In light of the new Regulations, this section therefore examines both rights, in order to determine how they might be affected.

(i) Data Protection

According to Article 5 of the General Data Protection Regulation,[212] before personal data can be processed legally, a number of principles need to be complied with. These are: (a) lawfulness, fairness and transparency; (b) purpose limitation; (c) data minimisation; (d) data accuracy; (e) storage limitation; (f) data integrity and confidentiality; and (g) accountability.

The Interoperability Regulations raise a number of issues regarding compliance with these data protection principles, not least in relation to fairness and transparency (by extending the scope of the actors who can access the respective databases, highlighted above), purpose limitation, data minimisation (due to the vast scope of the personal data collected through the various databases and which can consequently be accessed through interoperability tools such as the CIR), data accuracy (addressed below) and storage limitation (by not clearly specifying the methods and timescales through which unnecessary data will be deleted).[213] However, for the purpose of this section, the principle of purpose limitation shall be focused on.

The principle of purpose limitation requires that when personal data is collected it is done so for *'specified, explicit and legitimate purposes'*[214] and is not *'further processed in a manner [which] is incompatible with those purposes.'*[215] The Interoperability Regulations violate this principle in at least two important ways.

Firstly, as has been referenced to already, each of the large-scale databases have been created for their own specific purpose and seek to achieve a set of specific objectives.[216] In justifying the necessity of the Interoperability Regulations, the Commission has repeatedly emphasised that the Regulations are purely intended to provide tools through which the objectives of Interoperability can be achieved, rather than to create new powers. However, the Regulations introduce no less than seven new objectives, which are not mentioned previously in the existing Regulations.[217] Rather than being purely technical, the Interoperability Regulations in fact seek to add new purposes through which personal data

[212] Regulation (EU) 2016/679.
[213] Casagran (n 73), 443-448.
[214] Art 5(1)(b), Regulation (EU) 2016/679.
[215] *Ibid.*
[216] Casagran (n 73).
[217] *Ibid.*

can be processed, such as identity fraud.[218] In order to fully comply with the principle of purpose limitation, it will therefore be necessary for these underlying databases to be reformulated in order to take account of these new purposes.[219]

The second interference relates to the increasingly blurred boundaries between the management of migration and the achievement of security related goals (which has been discussed in detail above).[220] While there are no doubt credible reasons for why it is important to enable the sharing of information between the spheres of migration and security, it should not be ignored that the original motivations behind these sets of databases are entirely different. Consider the examples of Eurodac (an asylum database) and VIS (an immigration database). Neither envisaged that the data contained within them would be accessed in a routine manner for law enforcement purposes.

Indeed, in both cases, the right to access data for law enforcement purposes was strictly restricted.[221] This is on account of the entirely different legal bases that exist between databases designed to facilitate the management of migration (VIS, Eurodac etc) and those which deal with law enforcement and judicial cooperation (SIS, ECRIS-TCN).[222] In many cases, it has become clear that data is being collected and stored for purposes beyond that which authorised their original collection.[223] The Interoperability Regulations amplify this effect through *'defin[ing] new purposes meant to justify the combination of information included in the policing and migration databases.'*[224] Such behaviour cannot be considered compatible with the principle of purpose limitation and is likely to constitute a disproportionate interference with the data protection rights of TCNs.[225]

(i) Privacy

The ECtHR has recognised that the systematic registration of personal data constitutes an interference with the right to private life, regardless of whether that information is subsequently used.[226] In order to be regarded as legitimate, it must be assessed against the requirements established within Article 8(2) ECHR, primarily whether this interference is: (a) in accordance with the law; (b) pursues a legitimate aim; and (c) is necessary in a democratic society.

Problems can be identified with all three requirements.

Firstly, in order to be classed as being *'in accordance with the law,'* it is necessary that the legislation justifying an interference is clear, foreseeable and adequately accessible.[227] Questions can be raised as to whether this is the case, particularly considering that: firstly,

[218] *Ibid.*

[219] Casagran (n 73); Gutheil et al (n 6).

[220] Casagran (n 73).

[221] Council Decision 2008/633/JHA; Regulation (EU) No 603/2013.

[222] EDPS (n 163).

[223] Aden (n 45); Curtin and Bastos (n 115).

[224] Aden (n 45), 103.

[225] Casagran (n 73); EDPS (n 163).

[226] Amann v Switzerland [2000] ECHR 88, para 69; Rotaru v Romania [2000] ECHR 192, para 46.

[227] Silver and Others v United Kingdom [1983] ECHR 5

some of the purposes justifying the collection and storage of personal data have no basis within the legislation establishing the underlying databases; and secondly, the Regulations establish the creation of three new databases in the form of the CIR, MID and BMS, despite this not being expressly acknowledged by the Commission.

Secondly, the requirement of necessity. While the achievement of the objectives presented within the Interoperability Regulations are no doubt important,[228] it can be questioned whether the introduction of the Interoperability Regulations is necessary to their achievement. There is little evidence to suggest that the current process of accessing the databases is substantially substandard, or that it causes great difficulties for the officials operating them.[229]

Finally, the proportionality of the Interoperability Regulations can also be questioned, particularly considering the fact that the personal data of a large number of individuals (after the EES and ETIAS come into operation, this will include every TCN who enters the territory of the EU, a number which is in the millions annually) shall be stored and subjected to processing through these provisions.[230] As becomes clear, the effects that the Interoperability Regulations can have for the rights to privacy and data protection are quite substantial.

5.6 How might other human rights be affected?

The effect these provisions have on human rights goes beyond simply the rights to privacy and data protection. In fact, a range of rights could be affected. However, for the purposes of this article, only two shall be considered.

Firstly, the right to non-discrimination, as protected under Article 14 of the ECHR and Article 21 of the EU Charter. These rights protect against discrimination on a range of grounds including sex, race, colour, language, religion, political or other opinion or national or social origin. In the context of the Interoperability Regulations, Article 20 of the Interoperability Regulations is particularly problematic, since it creates the risk of racial profiling, affecting not only TCNs but also EU citizens.[231] As mentioned previously, Article 20 provides police authorities with the power to carry out checks of the CIR in order to determine the identity of a person.[232] While limited to the specific situations listed in Article 20(1)(a)-(e), this is still a power which can be wielded widely by police authorities.

There is no restriction as to where these searches can be conducted, and consequently, searches of the CIR can also be conducted as part of a routine police stop. This creates a risk that the powers might be used discriminatorily, particularly against those who are determined as having *'suspicious'* characteristics, often on account of their race or physical

[228] Art 2, Reg (EU) 2019/817; Art 2, Reg (EU) 2019/818

[229] Casagran (n 73).

[230] Aden (n 45).

[231] Quintel (n 13); Vavoula (n 162).

[232] Reg (EU) 2019/817 and Reg (EU) 2019/818

appearance.[233] As has been seen with previous *'stop and search'* powers, it is likely that even despite the existence of non-discrimination provisions, the effect of these powers will be disproportionately felt on minority groups.[234] Additionally, the fact that these searches are conducted on the basis of an individual's biometric characteristics makes them particularly invasive.[235]

Secondly, the issue of data quality is also a factor which cannot be overlooked. For a long time, concerns have been raised as to the quality of the data which is contained within these large-scale databases, particularly regarding fingerprints.[236] Thus, if the data within the siloed databases is not accurate, this then raises serious concerns for when it is aggregated through the interoperability framework. Potentially, this could lead to issues such as *'irregularities, wrongful matches, and a significant amount of false hits.'*[237] For instance, poor fingerprints might result in individuals being identified with either a red or yellow link within the MID, leading to them to be subjected to increased checks, enhanced suspicion or even being refused entry into the territory of the EU. In this regard, it is important to also highlight that following the revision of the SIS legal framework, when an individual is refused entry into the EU territory or subjected to an entry ban, it is now mandatory for an alert to entered into SIS.[238] Poor data quality is therefore an issue which could have serious consequences for an individual.

5.7 Are the losses to an individual's privacy greater or less than the gains for security officials*?*

The final point, therefore, is to consider the cumulative effect that these databases have on the rights of TCNs. As has been highlighted above, through the development of these large-scale IT systems, the EU has sought to control the mobility of TCNs through developing a system of generalised mass surveillance which records their presence and movements within the EU, regardless of the reasons behind their travel.[239] Even though they might pose no threat, TCNs find themselves falling within a *'series of concentric risk*

[233] Quintel (n 82).

[234] Tufyal Choudhury and Helen Fenwick, 'The Impact of Counter-Terrorism Measures on Muslim Communities' (2011) 25(3) International Review of Law, Computers and Technology 151; Gillan and Quinton v UK [2010] ECHR 28.

[235] Vavoula (n 13); Quintel (n 46).

[236] Evelien Brouwer, 'Interoperability and Interstate Trust: a Perilous Combination for Fundamental Rights' (EU Migration Blog, 11 June 2019) <http://eumigrationlawblog.eu/interoperability-and-interstate-trust-a-perilous-combination-for-fundamental-rights/> accessed 8 March 2021; Quintel (n 13).

[237] Quintel (n 13), 221.

[238] Art 24, Regulation (EU) 2018/1861 of 28 November 2018 on 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 (EU) No 1987/2006 [2018] OJ L 312/14.

[239] Mitsilegas and Vavoula (n 154); Vavoula (n 13).

filters'[240] designed to *'categorise and identify migrants.'*[241] Once under the surveillance of the EU's databases, the EU can *'sort… between bona fide and male fide,'*[242] assess individual TCNs for their level of dangerousness or preventively exclude those they find undesirable.[243]

While the VIS and Eurodac have been capturing the data of those who require a visa or who have applied for international protection for a long time, the addition of the new EES and ETIAS databases ensure that this surveillance scheme is also extended to those who are visa exempt. As a result, it is now likely that nearly every TCN who enters the EU will find themselves included within the new interoperability framework in some form.[244] Consequently, the personal data of huge numbers of innocent individuals will be captured, stored and subjected to processing within these systems. The EES and ETIAS, for instance, are recording data on individuals who are simply partaking in legitimate, everyday activities.[245]

In some cases, they even store data on individuals who are not even within the territory of the EU – the VIS, in particular, retains data on individuals regardless of whether their visa application has been granted, refused or revoked.[246] Such a situation runs the risk of casting TCNs under a *'cloud of permanent suspicion.'*[247] And as the CJEU noted in the cases of Digital Rights Ireland [2014] and Tele2 [2016], systems of generalised surveillance are *'likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.'*[248]

The interoperability provisions are therefore the final piece of the puzzle through which this generalised surveillance of TCNs is established. As Vavoula notes, *'[while] each database considered on its own may not qualify as establishing generalised and indiscriminate surveillance of movement,'*[249] when combined through interoperability tools such as the CIR, this is likely more than enough to qualify. The largest remaining gap preventing the wholesale surveillance of TCNs (the lack of information regarding visa-exempt TCNs) was finally closed through the adoption of the EES and ETIAS, while ECRIS-TCN will ensure that the criminal records of TCNs can be shared more efficiently. Interoperability, meanwhile, brings all this information together and operationalises it. Tools such as the ESP, BMS, CIR and MID ensure that regardless of which database someone is located in, the relevant authorities will be able to find them with the click of a

[240] Vavoula (n 2), 230.
[241] Vavoula (n 2), 230
[242] Vavoula (n 144), 25.
[243] *Ibid*.
[244] Vavoula (n 13); EDPS (n 163).
[245] Mitsilegas and Vavoula (n 154).
[246] Arts 5 and 13, Regulation (EC) No 767/2008; Mitsilegas and Vavoula (n 154).
[247] Vavoula (n 144), 25.
[248] Joined Cases C-293/12 Digital Rights Ireland and C-594/12 Seitlinger and Others [2014] ECLI:EU:C:2014:238, para 37; Joined Cases C-203/15 Tele2 Sverige and C-698/15 Watson and Others [2016] ECLI:EU:C:2016:970, para 100.
[249] Vavoula (n 162).

button, while the introduction of Article 20 enables this power to be wielded anywhere and against anyone the authorities desire.

As Dijstelbloem and Broeders highlight, it is through the establishment of borders that *'categories of difference and separation'*[250] are created. These borders seek to divide TCNs into one of three categories – those who are trusted (the accepted), those who are not (the denied), and those who are suspect (the suspected).[251] The trusted will face little trouble from border controls, while the distrusted will find themselves refused entry or apprehended. The final group, the suspect, is that which the vast majority of TCNs will fall within – these are the ones who will be subjected to additional scrutiny.[252]

The establishment of interoperability highlights this perfectly. Through the six underlying databases, the EU has already definitively drawn a line separating the treatment of TCNs (the suspect) from EU citizens (the trusted). The movement of TCNs is to be regulated, whereas the free movement of citizens must be guaranteed. However, with interoperability they have redrawn the lines – by redefining the distinction between *'safe'* and *'suspicious.'* The consequence of interoperability is the expansion of this final category. Whereas visa-exempt TCNs previously could class themselves within the first group, they are now seen as sliding into the third. It can therefore be suggested that the negative consequences for TCNs far outweigh the added benefits of establishing interoperability.

6. Conclusion

When the European Commission instigated the development of the Interoperability Regulations, they were motivated by a desire to address the *'complex landscape'* of large-scale databases which had developed within the fields of migration and security. However, in many ways it can be argued that rather than simply simplifying the process through which information can be exchanged, the European Commission has instead further complicated the matter, particularly in relation to the rights of TCNs. As the Commission has highlighted, the development of each database is tied to its own institutional, legal and political context and consequently the information is rarely interconnected between the various databases.[253]

While the EU sees this as problematic, it should be acknowledged that this is simply a consequence of the fact that each of the databases have been created for different purposes, reflected in their differing legal bases. While the objective of interoperability can be justified in some ways – interconnections between the databases would certainly be beneficial for more effective information sharing – this does not change the fact that considering the different purposes behind the various databases, simply lumping them together within an interoperable framework is problematic.

[250] Dijstelbloem and Broeders (n 68), 23.

[251] *Ibid* 32.

[252] *Ibid* 32.

[253] COM(2016) 205 final.

However, now that this has occurred, it offers an ample opportunity to emphasise why considering measures such as these from a more holistic perspective is important. Whenever a new measure such as interoperability is introduced, it is important to understand the consequences that such as action will have for the entire ecosystem of actors. In introducing their framework for interoperability, the Commission deals with the situation in too shallow a manner – by focusing only on promoting more efficient data access, it fails to consider the specific reasons behind why the measures were implemented. As an ecosystems approach highlights, rather than looking at the interoperability provisions in isolation, what should be sought is a greater understanding of the wider context in which these databases have developed.

Therefore, it is important to understand not only how these actors are interconnected, but also how they interact – an important element of the ecosystem concept. On account of their different legal basis and purposes, each database has their own network of actors to which it is connected – the exact make-up of these networks is influenced by the categories of information contained within each database, and the purposes behind its development. By considering the interoperability provisions in isolation, it fails to consider how the various national authorities engage with these databases, and how they can be used to enable interactions between the authorities of various member states. For example, in the case of Zaghba, while both Italy and the UK were using the same system, because of the different ways in which they had implemented it within their domestic sphere, the actors to which it was attached were different.

Consequently, the information did not get where it was supposed to go as a result of a failure to understand how the different actors were interconnected. While interoperability might streamline access to data, it will not necessarily have the consequence of making the '*complex landscape*' less complicated. Rather, it has resulted in the creation of new databases and data processing purposes which provide a method through which to increasingly monitor the movements of TCNs within the EU, at the expense of the protection of their human rights.