German Law Journal (2021), **22**, pp. 391–415
doi:10.1017/glj.2021.11

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Special Issue: Judicial and Extra-judicial Challenges in the EU Multi- and Cross-level Administrative Framework

Information Sharing in the Dublin System: Remedies for Asylum Seekers In-Between Gaps in Judicial Protection and Interstate Trust

Niovi Vavoula*

Lecturer in Migration and Security, Queen Mary University of London, London, England

(Received 19 March 2021; accepted 11 April 2021)

Abstract

In most EU policy areas, procedural cooperation between national administrations takes place through the shared implementation of "composite" decision-making procedures, facilitated by the operation of multijurisdictional networks or horizontal or vertical information exchange. In the context of asylum policy, such administrative cooperation has been necessary in the distribution of asylum seekers—in accordance with the Dublin III Regulation, which allocates responsibility among Member States to examine an asylum application. In addition to rules in the Regulation itself—Article 34—information sharing also takes place through Eurodac, an EU-wide centralized information system. This Article examines whether the Dublin system ensures effective judicial and administrative remedies in the operationalization of multijurisdictional information networks. It analyzes the relevant Eurodac and Dublin-related legislation, national implementation, and national case law through the lens of administrative cooperation. The assumption that the data exchanged has been acquired and processed lawfully, due to interstate trust, and the extent to which that assumption is rebuttable, are central themes throughout this Article. It is argued that administrative cooperation through information sharing takes precedence over the right to an effective remedy, and that, in practice, judicial and extrajudicial remedies are insufficient to protect asylum seekers.

Keywords: Eurodac; Dublin system; information sharing; composite procedure; asylum seekers

A. Introduction

Much ink has been spilled on the need for cooperation among public administrations in the European Union (EU) in order to face the emerging challenges of the material application of EU law, to the extent that such cooperation has become the "backbone of the EU's unique system of government and governance."[1] The principle of administrative cooperation, constitutionalized in Article 4(3) of the Treaty on the European Union (TEU) and Article 197 of the Treaty on the

*This Article is a deliverable of the MAPS Project, funded as Jean Monnet Network (2019–2021) 599856-EPP-1–2018-1-IT-EPPJMO-NETWORK, Grant decision 2018–1606/001–001. I am grateful to Anne Sheridan for drawing my attention to the case of *BS and RS v. Refugee Appeals Tribunal and Ors* and Evelien Brouwer for her valuable help in finding cases *Rb Den Haag December 10, 2019, NL19.24439, JV 2020/59, ve19003512* and *ABRvS April 11, 2019, AR 2019/106, ve19001150*. I also thank Evangelia (Lilian) Tsourdi for her useful comments in the development of this Article. Any errors remain my own.

[1]*See* Alexander H. Türk & Herwig C.H. Hofmann, *An Introduction to EU Administrative Governance*, *in* EU ADMINISTRATIVE GOVERNANCE 1 (Alexander H. Türk & Herwig C.H. Hofmann eds., 2006).

Functioning of the European Union (TFEU), entails that national administrations are increasingly required to interact with one another in various ways.[2] In most EU policy areas, the procedural cooperation between national administrations materializes through the shared implementation of "composite" decision-making procedures[3]—facilitated by the operation of multijurisdictional networks[4]—or through extensive horizontal or vertical information exchanges.[5] To that end, domestic authorities may be required to collect, generate, and transfer information to their counterparts in other Member States as preparatory measures to decision-making and enforcement activities. On the basis of such information, Member States—or even EU bodies and institutions—may adopt acts or take decisions.

The architecture of information networks has been developed in a policy-specific fashion and asylum policy follows that path, albeit with its own intricacies. The purpose of Article 78(2) TFEU is to develop a "common European asylum system" (CEAS), which has led to the elaboration of different legislative harmonization measures concerning the definition of who qualifies as a refugee or a beneficiary of subsidiary protection,[6] common procedures for the examination of asylum claims,[7] and reception conditions that should be afforded to asylum seekers during the examination of their claims.[8] At present, the centerpiece of the CEAS is the Dublin III Regulation,[9] an assignation mechanism to identify the Member State responsible for examining a specific asylum claim through an array of hierarchical criteria. It is in the distribution of asylum seekers, in accordance with the responsibility-allocation scheme, that administrative cooperation in the form of information sharing is necessary. Such information sharing takes place through two main avenues. First, an EU-wide centralized information system called Eurodac has been set up precisely to assist Member States in assigning each asylum seeker to the responsible Member State through the joint gathering of information.[10] Second, the Dublin III Regulation itself, in particular Article 34, organizes the manner in which further information sharing may take place, in order to determine the responsible Member State or to arrange the transfer of an asylum applicant.

In a complex area of multi-layered actorness, the availability of effective remedies either ex-post—judicial review—or throughout the process—administrative review—is crucial to

[2]*See* Micaela Lottini, *From "Administrative Cooperation" in the Application of European Union Law to "Administrative Cooperation" in the Protection of European Rights and Liberties*, 18 EUR. PUB. L. 127, 128 (2012).

[3]*See* Herwig C.H. Hofmann, *Composite Procedures in EU Administrative Law*, *in* LEGAL CHALLENGES IN EU ADMINISTRATIVE LAW: TOWARDS AN INTEGRATED ADMINISTRATION 136–67 (Herwig C.H. Hofmann & Alexander H. Türk eds., 2009).

[4]*See* Herwig C.H. Hofmann & Morgane Tidghi, *Rights and Remedies in Implementation of EU Policies by Multi-Jurisdictional Networks*, 20 EUR. PUB. L. 147, 148 (2014).

[5]*See* Jens-Peter Schneider, *Basic Structures of Information Management in the European Administrative Union*, 20 EUR. PUB. L. 89, 91 (2014).

[6]Directive 2011/95, of the European Parliament and of the Council of 13 December 2011 on Standards for the Qualification of Third-Country Nationals or Stateless Persons as Beneficiaries of International Protection, for a Uniform Status for Refugees or for Persons Eligible for Subsidiary Protection, and for the Content of the Protection Granted, 2011 O.J. (L 337) 9 (EU).

[7]Directive 2013/32, of the European Parliament and of the Council of 26 June 2013 on Common Procedures for Granting and Withdrawing International Protection, 2013 O.J. (L 180) 60 (EU).

[8]Directive 2013/33, of the European Parliament and of the Council of 26 June 2013 Laying Down Standards for the Reception of Applicants for International Protection, 2013 O.J. (L 180) 96 (EU).

[9]Regulation 604/2013, of the European Parliament and of the Council 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 (Recast), 2013 O.J. (L 180) 31 (EU) [hereinafter Dublin III Regulation].

[10]*See* Regulation 603/2013, of the European Parliament and of the Council of 26 June 2013 on the Establishment of "Eurodac" for the Comparison of Fingerprints for the Effective Application of Regulation 604/2013 Establishing the Criteria and Mechanisms for Determining the Member State Responsible for Examining an Application for International Protection Lodged in One of the Member States by a Third-Country National or a Stateless Person and on Requests for the Comparison with Eurodac Data by Member States' Law Enforcement Authorities and Europol for Law Enforcement Purposes, and Amending Regulation 1077/2011 Establishing a European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, 2013 O.J. (L 180) 1 (EU) [hereinafter Recast Eurodac Regulation].

https://doi.org/10.1017/glj.2021.11 Published online by Cambridge University Press

ensure the protection of individual rights and accountability in the exercise of public powers.[11] The existence and effectiveness of remedies at the disposal of asylum seekers has attracted scholarly attention, albeit the emphasis has been either on other CEAS legal instruments or, where the Dublin system is scrutinized, on the application of the hierarchical allocation criteria.[12] Thus, the rules on information sharing have so far been off the academic radar. As a result, the question of whether the Dublin system ensures effective judicial and administrative remedies in the operationalization of multijurisdictional information networks has not been addressed.

This Article aims at filling this gap in the literature by analyzing the relevant Eurodac and Dublin-related legislation, national implementation, and national case law through the lens of administrative cooperation. To that end, the next section provides a concise synopsis of the Dublin III Regulation to lay the foundation for the subsequent analysis. Then, this Article explores the case of Eurodac in relation to the availability and effectiveness of remedies for asylum seekers, both extrajudicial and judicial. The following section is devoted to the challenges of the rules of the Dublin III Regulation concerning administrative cooperation, in the form of information exchange for the right to an effective remedy, as enshrined in Article 47 of the EU Charter of Fundamental Rights (Charter). The assumption that the data exchanged has been acquired and processed lawfully, due to interstate trust, and the extent to which that assumption is rebuttable are central themes throughout this Article. It is argued that administrative cooperation through information sharing takes precedence over the right to an effective remedy and that, in practice, judicial and extrajudicial remedies are insufficient to protect asylum seekers. This Article concludes with a summary of the main findings.

B. The Dublin System: A Sketch

The ongoing harmonization of national rules on asylum procedure, as aforementioned, does not signify that asylum applications in the EU are examined through a common asylum procedure or that there is a uniform status for those granted asylum within the EU.[13] Asylum applications are still examined by individual Member States following a national asylum procedure and result in national refugee status. Without centralization, national systems are meant to interact with each other to govern asylum flows and allocate responsibility for asylum seekers through the so-called Dublin system.

The Dublin system was initially established through the 1990 Dublin Convention,[14] outside the EU framework. The Convention was signed as a corollary to the abolition of intra-Member State border controls and the need for a coordinated response to the increasing logistical demands which the operation of the asylum system placed upon Member States. In particular, it aimed at providing a clear set of common rules to determine which Member State would be responsible for examining an asylum application—in cases of potentially overlapping asylum claims in different countries—as a result of the phenomena of "refugees in orbit"[15] and "forum shopping."[16]

[11]*See* Hofmann & Tidghi, *supra* note 4, at 152.

[12]*See, e.g.*, Marcelle Reneman, EU Asylum Procedures and the Right to an Effective Remedy (2014); Evangelia (Lilian) Tsourdi, *Of Legislative Waves and Case Law: Effective Judicial Protection, Right to an Effective Remedy and Proceduralisation in the EU Asylum Policy*, 12 Rev. Eur. Admin. L. 143 (2019).

[13]Already in 1999, in its Tampere Conclusions the European Council stated that "[i]n the longer term, Community rules should lead to a common asylum procedure and a uniform status for those who are granted asylum throughout the Union." *See* Presidency Conclusions, Tampere European Council (Oct. 15–16, 1999), para. 15, https://www.europarl.europa.eu/summits/tam_en.htm#c.

[14]Convention Determining the State Responsible for Examining Applications for Asylum Lodged in One of the Member States of the European Communities, June 15, 1990, 1997 O.J. (C 254) 1 [hereinafter Dublin Convention].

[15]*See* Göran Melander, Refugees in Orbit (1978).

[16]For elaboration of this point, see ECJ, Joined Cases 411 & 493/10, N.S. v. Sec'y of State for the Home Dep't, ECLI:EU:C:2011:865 (Dec. 21, 2011), para. 79, https://curia.europa.eu/juris/document/document.jsf?text=&docid=117187&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=5742659.

https://doi.org/10.1017/glj.2021.11 Published online by Cambridge University Press

The Convention has been amended twice and—at the time of writing the Dublin III Regulation is in force[17] allocates responsibility within the CEAS, all the while introducing and reinforcing substantive individual rights and procedural safeguards. The regulation is premised on the "single application" principle, according to which an application must be heard by a single Member State.[18] To determine which Member State is responsible for examining each application, the regulation prescribes an allocation mechanism comprising a hierarchy of criteria.[19] Such criteria include the existence of a family member of the applicant who is a recognized refugee or an asylum applicant in another Member State,[20] whether a certain Member State has issued the applicant with a residence permit or a visa,[21] and the rule that the responsible party will be the Member State from where the asylum seeker first entered the EU.[22] In practice, the "first country of entry" rule is the main criterion used by Member States' authorities. Guild has observed that the responsibility for examining an asylum claim has thus been treated "as a burden and a punishment for the Member State which permitted the individual to arrive in the Union."[23] Where asylum seekers are present in the territory of a Member State other than the responsible Member State, they are to be transferred to the latter, unless limited exceptions apply.[24] Transfers are to take place either because the asylum seeker has first applied to the responsible Member State—a "take back" request[25]—or because the asylum seeker ought to have applied there—a "take charge" request[26]—but unauthorized secondary movement took place.

A wealth of academic commentators have criticized how the Dublin system creates an asymmetrical burden and is largely unconcerned with fair sharing of responsibility among the Member States, as that responsibility is largely dependent upon the geographical locus of each State.[27] Another line of authors view the Dublin system as embodying the principle of negative mutual recognition and the introduction of automaticity among Member States. Indeed, the occurrence of one of the Dublin criteria creates a duty for one Member State to "take charge" or "take back" an asylum seeker and thus recognize the refusal of another Member State—which transfers the asylum seeker in question—to examine the asylum application.[28] Transfers in that context are based on interstate mutual trust, under the presumption that the receiving state provides an equivalent level of human rights protection to asylum seekers as the sending state.[29]

From an administrative law standpoint, the determination of the responsible Member State requires intense horizontal transnational cooperation among national administrations to track down the possible intervention of another jurisdiction. The national administrations involved may not organically belong to the same unit, directory, or even legal system. For instance, to

[17]*See* Dublin III Regulation, *supra* note 9; *Commission Proposal for a Regulation of the European Parliament and of the Council on Asylum and Migration Management and Amending Council Directive 2003/109 and the Proposed Regulation XXX/XXX [Asylum and Migration Fund]*, COM (2020) 610 final (Sept. 23, 2020) [hereinafter *Proposed Regulation on Asylum and Migration Management*].

[18]*See* Dublin III Regulation, *supra* note 9, at art. 3(1).

[19]*See id.* at art. 7.

[20]*See id.* at arts. 9–11.

[21]*See id.* at art. 12.

[22]*See id.* at art. 13.

[23]Elspeth Guild, *The Europeanisation of Europe's Asylum Policy*, 18 Int'l J. Refugee L. 630, 637 (2006).

[24]*See* Dublin III Regulation, *supra* note 9, at art. 17.

[25]*See id.* at arts. 23–24.

[26]*See id.* at arts. 21–22.

[27]*See, e.g.*, Francesco Maiani, *The Dublin III Regulation: A New Legal Framework for a More Humane System?*, *in* Reforming the Common European Asylum System: The New European Refugee Law 104–14 (Vincent Chetail et al. eds., 2016).

[28]*See* Elspeth Guild, *Seeking Asylum: Storm Clouds Between International Commitments and EU Legislative Measures*, 29 Eur. L. Rev. 198 (2004).

[29]*See* Valsamis Mitsilegas, *Solidarity and Trust in the Common European Asylum System*, 2 Comp. Migration. Stud. 181, 184 (2014).

https://doi.org/10.1017/glj.2021.11 Published online by Cambridge University Press

determine whether a Member State has issued a Schengen (short-stay) visa to an asylum seeker, national administrations may consult the designated Schengen-wide centralized information system—the Visa Information System (VIS)—to check whether a record therein exists, indicating the issuance of a visa by another administrative authority.[30] To that end, the Dublin system embraces various procedures of administrative cooperation for its functioning, which at least partly encompass composite elements. A single administrative decision on the territorial belonging of an asylum applicant and their consequent transfer to the responsible Member State may involve multiple jurisdictions and be grounded on the input by national administrations which interact and/or cooperate via established information networks. The processing of information in this context is crucial in view of the abovementioned principles of "single application" and mutual recognition. A prime example of an advanced form of composite information management is Eurodac, a Europe-wide[31] centralized information system which has been established as a support tool of the Dublin system to determine whether a Member State is responsible for the presence of an asylum applicant.

C. The Eurodac Database: The Digital Sidekick of the Dublin System

Eurodac (European Dactyloscopic System) constitutes an integral, yet relatively under-explored component of the CEAS.[32] It forms part of an elaborate network of Europe-wide centralized information systems that process various categories of personal data collected from different categories of third-country nationals. Eurodac functions alongside two other operational information systems—namely the Schengen Information System (SIS)[33] and the VIS[34]—all of which are managed by eu-LISA, the EU agency for the operational management of large-scale information systems.[35]

I. The Recast Eurodac Regulation in a Nutshell

Already in the early stages of Dublin cooperation, discussions revolved around the possibility of setting up a European system to compare the dactyloscopic data of asylum seekers[36] with the underlying aim of tracking possible onward movements of asylum seekers in other Member States and preventing abuse of the system by the submission of several applications for asylum by one person. Eurodac was established via Regulation 2725/2000[37] and complemented by

[30] *See* Regulation 767/2008, of the European Parliament and of the Council of 9 July 2008 Concerning the Visa Information System (VIS) and the Exchange of Data Between Member States on Short-Stay Visas, 2008 O.J. (L 218) 60 (EC).; *see also infra* Section D.

[31] All EU Member States are connected to the system, including Ireland and—for the moment—the United Kingdom. Norway, Iceland, Switzerland, and Liechtenstein are Dublin Associate States and, therefore, are connected to Eurodac as well.

[32] For a holistic analysis of Eurodac, see Niovi Vavoula, Immigration and Privacy in the Law of the European Union: The Case of Information Systems ch. 4 (forthcoming 2021).

[33] *See* Regulation 2018/1861, of the European Parliament and of the Council of 28 November 2018 on the Establishment, Operation and Use of the Schengen Information System (SIS) in the Field of Border Checks, and Amending the Convention Implementing the Schengen Agreement, and Amending and Repealing Regulation 1987/2006, 2018 O.J. (L 312) 14 (EU).

[34] *See* Regulation 767/2008, *supra* note 30.

[35] *See* Regulation 2018/1726, of the European Parliament and of the Council of 14 November 2018, on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and Amending Regulation 1987/2006 and Council Decision 2007/533/JHA and Repealing Regulation 1077/2011, 2018 O.J. (L 295) 99 (EU) [hereinafter eu-LISA Regulation]. In the future, three more centralized information systems will be operational: The Entry/Exit System, the European Travel Information and Authorisation System (ETIAS), and the European Criminal Record Information Systems (ECRIS).

[36] For an account of the Eurodac story, see Jonathan Aus, *Eurodac: A Solution Looking for a Problem?*, 10 Eur. Integration Online Papers 1 (2006).

[37] *See* Council Regulation 2725/2000 of Dec. 11, 2000, Concerning the Establishment of "Eurodac" for the Comparison of Fingerprints for the Effective Application of the Dublin Convention, 2000 O.J. (L 316) 1 (EC).

https://doi.org/10.1017/glj.2021.11 Published online by Cambridge University Press

Regulation 407/2002.[38] The Eurodac rules were recast in 2013, primarily to add the use of Eurodac fingerprints for the prevention, detection, and investigation of terrorist offenses and other serious crimes as an ancillary purpose of the system.[39] That said, at the time of writing, the primary objective of Eurodac is to support the implementation of the Dublin system. As a response to the so-called "refugee crisis," a recast Eurodac proposal was adopted in 2016 to reconfigure the system as a tool for wider migration purposes.[40] On September 23, 2020, a revised Eurodac proposal[41] was adopted in the framework of the New Pact for Migration and Asylum,[42] proposing that Eurodac would serve asylum, resettlement, and irregular migration purposes.[43]

Despite its reconfigurations, Eurodac has been intrinsically linked to the allocation of the Member State responsible for the examination of an application for international protection. Article 1 of the recast Eurodac Regulation stipulates that the purpose of the information system is:

> [T]o assist in determining which Member State is to be responsible pursuant to Regulation (EU) No. 604/2013 for examining an application for international protection lodged in a Member State, and otherwise to facilitate the application of the Regulation (EU) No. 604/2013 under the conditions set out in this Regulation.[44]

Eurodac requires Member States to promptly collect a full set of the fingerprints of every applicant for international protection over the age of fourteen.[45] The collected fingerprints are transmitted and stored in the Central System, a database managed by eu-LISA, where they are automatically compared with fingerprints that have already been transmitted and stored by other participating countries.[46] Eurodac is equipped with an Automated Fingerprint Identification System (AFIS) and functions on a hit/no hit basis; in case of a match, a notification is given.[47] Furthermore, Member States are under the obligation to collect the fingerprints of all third-country nationals apprehended "in connection with the irregular crossing by land, sea or air" of the Member State

[38]*See* Council Regulation 407/2002 of Feb. 28, 2002, Laying Down Certain Rules to Implement Regulation 2725/2000 Concerning the Establishment of "Eurodac" for the Comparison of Fingerprints for the Effective Application of the Dublin Convention, 2002 O.J. (L 62) 1 (EC).

[39]*See* Recast Eurodac Regulation, *supra* note 10. For an analysis, see Niovi Vavoula, *The Recast Eurodac Regulation: Are Asylum Seekers Treated as Suspected Criminals?*, *in* SEEKING ASYLUM IN THE EUROPEAN UNION: SELECTED PROTECTION ISSUES RAISED BY THE SECOND PHASE OF THE COMMON EUROPEAN ASYLUM SYSTEM 247–73 (Céline Bauloz et al. eds., 2015).

[40]*See 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 604/2013, Establishing the Criteria and Mechanisms for Determining the Member State Responsible for Examining an Application for International Protection Lodged in One of the Member States by a Third-Country National or a Stateless Person for Identifying an Illegally Staying Third-Country National or Stateless Person and on Requests for the Comparison with Eurodac Data by Member States' Law Enforcement Authorities and Europol for Law Enforcement Purposes (Recast)*, COM (2016) 272 final (May 23, 2016) [hereinafter *Recast Eurodac Proposal*]. An inter-institutional agreement between the co-legislators was reached in 2019.

[41]*See Commission Amended Proposal of a Regulation of the European Parliament and of the Council on the Establishment of "Eurodac" for the Comparison of Biometric Data for the Effective Application of Regulation XXX/XXX [Regulation on Asylum and Migration Management] and of Regulation XXX/XXX [Resettlement Regulation], 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 and Amending Regulations 2018/1240 and 2019/818*, COM (2020) 614 final (Sept. 23, 2020).

[42]*Commission Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, COM (2020) 609 final (Sept. 23, 2020).

[43]For an analysis, see Niovi Vavoula, *The Transformation of Eurodac Under the New Pact on Migration and Asylum: From the Sidekick of the Dublin System to a Database in Support of EU Policies on Asylum, Resettlement and Irregular Migration* (Eur. Council on Refugees & Exiles, Working Paper, 2021).

[44]See Recast Eurodac Regulation, *supra* note 10, at art. 1.

[45]*See* Recast Eurodac Regulation, *supra* note 10, at art. 9(1).

[46]*See* Recast Eurodac Regulation, *supra* note 10, at art. 9(3).

[47]*See* Recast Eurodac Regulation, *supra* note 10, at art. 9(5).

https://doi.org/10.1017/glj.2021.11 Published online by Cambridge University Press

and transmit them to the Central System for comparison against fingerprints that will subsequently be collected from asylum seekers.[48] This is to ensure that persons who were apprehended irregularly crossing the EU external border and subsequently apply for international protection in another Member State could be allocated to the responsible Member States in accordance with the "first country of entry" rule. A third category of third-country nationals whose fingerprints are collected includes "persons found illegally staying in a Member State."[49] Nevertheless, for now, neither are Member States obliged to undertake the procedure nor is the data centrally stored.[50] Overall, fingerprinting—in relation to both of these categories of third-country nationals—is meant to assist in determining whether the individual in question has first entered through a specific Member State, so as to enforce the Dublin rules. If a Eurodac check reveals that the fingerprints were already recorded in another Member State—a "hit"—it will establish whether the applicant has already lodged an application for international protection in that other Member State, or whether the applicant has irregularly transited through that other Member State. Consequently, the latter Member State may be requested to take back or charge the asylum applicant, in accordance with the Dublin III Regulation.[51]

Apart from a full set of fingerprints, Eurodac stores limited information on the sex of asylum seekers and irregular border crossers, the date of registration and transmission of fingerprints to the Central Unit, and the Member State of origin.[52] Details on the person's name, nationality, or date of birth—as well as other information, such as special needs or occupation—are not included, but are collected and processed by national authorities in accordance with their domestic legislation. When there is a hit, the data is transferred through the DubliNet system, an electronic communication network set-up under Article 18 of the Dublin III Regulation, enabling information sharing between the national authorities dealing with asylum applications. The two involved Member States may exchange personal data—other than the limited data set stored in Eurodac through DubliNet, in accordance with Article 34 of the Dublin III Regulation—which is analyzed below.[53] As a result, although Eurodac fingerprinting does not determine the identity of a person per se, it contributes to their identification. A link may be established between an asylum applicant and a past Eurodac entry, which is verifiable through information sharing between the state that conducts the check and the state of past Eurodac entry.[54] Furthermore, Article 1(3) of the recast Eurodac Regulation allows the Member State of origin to cross-check the Eurodac fingerprints against other databases established under national law, thus leading to the identification of the person. As a result, Eurodac operates as a de facto quasi-identification tool, though strictly speaking at the time of writing, identification does not feature among the objectives of the system. However, Article 1(1)(e) of the amended Eurodac proposal prescribes that the system will assist in the correct identification of persons registered.

II. Presumptions and Trust in a Digitalized Environment

From an operational perspective, Eurodac constitutes the first experiment of the EU with biometric identifiers—specifically fingerprints—and the largest multijurisdictional information system worldwide, functioning in thirty-two European countries.[55] According to the latest statistics, in

[48]*See* Recast Eurodac Regulation, *supra* note 10, at arts. 14–16.

[49]*See* Recast Eurodac Regulation, *supra* note 10, at art. 17.

[50]The 2020 Commission Proposal foresees the storage of such data. *See Recast Eurodac Proposal*, *supra* note 40, at art. 2.

[51]*See supra* Section B.

[52]*See* Recast Eurodac Regulation, *supra* note 10, at arts. 11, 14(2).

[53]*See infra* Section D.

[54]Eur. Union Fundamental Rights Agency, Fundamental Rights Implications of the Obligation to Provide Fingerprints for Eurodac 3 (2015), https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-fingerprinting-focus-paper_en.pdf.

[55]*See supra* note 31.

https://doi.org/10.1017/glj.2021.11 Published online by Cambridge University Press

2019, Member States successfully transmitted a total of 916,577 sets of fingerprints.[56] As the authorities participating in Eurodac are granted direct information access to stored data for all participating authorities, the system establishes a high level of information integration and constitutes an example of the most advanced form of information sharing.[57] By organizing the joint gathering of information by Member States, Eurodac constitutes a prime example of a composite procedure, whereby the administrative procedure of allocating the responsible Member State in accordance with the Dublin rules is supported by information transferred to it by other Member States—horizontal cooperation—and assisted by an EU agency, eu-LISA—vertical cooperation.[58]

Eurodac functions as the necessary corollary of the Dublin system. The latter cannot run smoothly unless Member States can reliably verify whether a person has already applied for international protection or was apprehended in connection with the irregular crossing of an external border in another participating State. In case of a hit, the administrative authorities *presume* that at the time when the Eurodac record was inserted, the individual in question either filed an asylum claim or was an irregular migrant—and thus the responsibility for the applicant lies with another Member State. This presumption is based on the existence of a technology-based trust that operates on two levels. First, there exists interstate trust among national administrations that the fingerprints are lawfully and carefully collected and transmitted, the rights of the fingerprinted third-country nationals are safeguarded, and the record entered in Eurodac is accurate, of high quality, up-to-date, and compliant with the rights to dignity,[59] respect for private life,[60] and personal data protection.[61] In addition, Eurodac exemplifies trust among Member States in overseeing the external borders of the EU by zealously fingerprinting irregular entrants. Second, interstate trust in procedures is facilitated by trust in technology and the belief that biometric identifiers, including fingerprints, along with their centralized storage are trustworthy advents. As a result, the existence of Eurodac allows trust to build among participating States. Eurodac is simultaneously a result of and a tool for fostering interstate trust in the CEAS. Undoubtedly, biometric identifiers have been heralded as revolutionary tools that present a series of attractive characteristics due to their universality, distinctiveness, and permanence.[62] Their reliable nature has been confirmed by the Court of Justice of the European Union (CJEU) in *Schwarz*—concerning the inclusion of two fingerprints in EU biometric passports—with the CJEU holding that "the fact that the method is not wholly reliable is not decisive."[63] Article 22 of the Dublin III Regulation, as elaborated in Commission Implementing Regulation 118/2014,[64] distinguishes between probative and circumstantial evidence of a Member State's responsibility, with Eurodac hits falling within the former category. The reliability of fingerprint identification is further manifested in the practical implementation of the Dublin rules, whereby a Eurodac hit constitutes the primary proof on the basis of which a Dublin transfer may occur.[65] Crucially, some Member States, particularly those who receive take back requests, only accept Eurodac hits.[66]

[56]*See* EU-LISA, EURODAC – 2019 STATISTICS, at 5 (2020), https://www.eulisa.europa.eu/Publications/Reports/Eurodac-2019Statistics.pdf.

[57]*See* Schneider, *supra* note 5, at 89–90.

[58]*See* SERGIO ALONSO DE LEON, COMPOSITE PROCEDURES IN THE EUROPEAN UNION 209–10 (2017); *see also* Hofmann, *supra* note 3, at 138–39.

[59]*See* Charter of Fundamental Rights of the European Union art. 1, Oct. 26, 2012, 2012 O.J. (C 326) 391.

[60]*See id.* art. 7.

[61]*See id.* art. 8.

[62]*See, e.g.*, ELS KINDT, PRIVACY AND DATA PROTECTION ISSUES OF BIOMETRICS APPLICATIONS (2013).

[63]ECJ, Case C-291/12, Schwarz v. Stadt Bochum, ECLI:EU:C:2013:670 (Oct. 17, 2013), para. 43, http://curia.europa.eu/juris/liste.jsf?num=C-291/12.

[64]Commission Implementing Regulation 118/2014, of 30 January 2014 Amending Regulation 1560/2003, Laying Down Detailed Rules for the Application of Council Regulation 343/2003, Establishing the Criteria and Mechanisms for Determining the Member State Responsible for Examining an Asylum Application Lodged in One of the Member States by a Third-Country National, 2014 O.J. (L 39) 1 (EU).

https://doi.org/10.1017/glj.2021.11 Published online by Cambridge University Press

Scratching below the surface of a seemingly seamless system, trust—both interstate and to modern technologies—is not a bed of roses. First, particularly since 2015—when refugees and migrants entered the EU *en masse*—it has been reported that in certain Member States, failure to comply with their Eurodac obligations—particularly in relation to the obligation to transmit the relevant data to the Central System within seventy-two hours—became a frequent phenomenon attributed to infrastructure deficiencies or the unwillingness of State authorities to take responsibility for asylum seekers.[67] Failure to fingerprint was thus utilized by certain Member States as a means to protest the unfairness of the Dublin system and consequently to evade their responsibilities. These deficiencies persist to date. In its audit on EU information systems, the European Court of Auditors reported that fifteen countries exceeded the prescribed time limit. It gave—as an example—the case of Spain, in which the transmission of fingerprints to Eurodac may take up to thirty days, thus leaving a person apprehended during an irregular border crossing into Spain a significant amount of time to reach another Member State and apply for asylum there.[68] In that sense, Eurodac actually undermines trust among Member States. Second, biometric identifiers constitute a special category of personal data under the General Data Protection Regulation (GDPR), thus requiring increased safeguards.[69] Third, the untested belief of the fallibility of biometric identifiers has been questioned by numerical evidence. It has been reported that 16% of inquiries in Eurodac resulted in a hit. In 10% of those cases, the biographic data was found to be inadequate, and in 4.5% of cases, the quality of the fingerprint acquired was too weak.[70] Overall, 28,195 data sets were rejected by the Central System due to insufficient quality.[71] This is not surprising, as much ink has been spilled on the data quality issues experienced in information systems, including Eurodac—due to spelling errors, lack of documentation, insufficient language skills, technical deficiencies, incorrect transcription of names into the Latin alphabet, recording of birth dates when the precise date is unknown, or lack of training.[72] Fourth, Member States have reported challenges when multiple Eurodac hits have been available, thus cancelling the probative nature of the hit. In certain cases, the lack of trust between Member States preexists and a hit may not result in a transfer, as certain Member States assume responsibility in accordance with Article 7 of the Dublin III Regulation.[73] Finally, despite the aforementioned challenges, reliance on modern technologies has led—in certain cases—to the prioritization of a Eurodac check over the investigation of family ties, thus jeopardizing the hierarchy of the Dublin criteria.[74]

In light of the above, a question emerges: In an era of trust in modern technologies and administrative cooperation, what remedies are available for asylum seekers when their personal

[65]European Commission, *Evaluation of the Implementation of the Dublin III Regulation - Final Report*, at 25 (March 18, 2016), https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/asylum/examination-of-applicants/docs/evaluation_of_the_implementation_of_the_dublin_iii_regulation_en.pdf.

[66]*Id.* at 25–26.

[67]For an account of such deficiencies in Greece, see *More Than a Third of Migrants Not Fingerprinted, Officials Say*, EKATHIMERINI (Aug. 20, 2015, 10:42 AM), http://www.ekathimerini.com/200728/article/ekathimerini/news/more-than-a-third-of-migrants-not-fingerprinted-officials-say.

[68]European Court of Auditors, *EU Information Systems Supporting Border Control - A Strong Tool, But More Focus Needed on Timely and Complete Data*, at 34–35 (2019), https://www.eca.europa.eu/Lists/ECADocuments/SR19_20/SR_Border_control_EN.pdf.

[69]Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, art. 9, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

[70]*Eurodac: The European Union's First Multinational Biometric System*, THALES (May 23, 2020), https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/eurodac.

[71]*See* eu-LISA Regulation, *supra* note 35, at 9, 16.

[72]*See* European Union Agency for Fundamental Rights, *Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights*, at 81–94 (2018), https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf.

[73]*See* European Commission, *supra* note 65, at 36.

[74]*Id.* at 31.

https://doi.org/10.1017/glj.2021.11 Published online by Cambridge University Press

information is collected and further processed? The existence and effectiveness of such remedies are crucial in view of the adverse consequences that unlawful information sharing may have on their status; they may face transfer to another Member State, which may have very diverse refugee recognition rates.[75] There exists a two-tier remedy system for individuals whose fingerprints are processed in Eurodac: Extrajudicial, via recourse to national data protection authorities as the supervisory authorities of Eurodac, and judicial, by bringing an action before national courts. The following sections discuss these remedies in turn.

III. Extrajudicial Remedies: Of Administrative Supervision and Individual Rights

The development of nonjudicial, administrative remedies as a means of resolving disputes concerning information processing without the intervention of a national court has been fostered since the inception of EU data protection law.[76] The focal points are the national data protection authorities (DPAs), which—according to Article 8(3) of the Charter and Article 16 TFEU—ensure compliance with data protection rules. Rules on the extrajudicial remedies in connection to Eurodac are found in the GDPR, which constitutes the *lex generalis*, and the recast Eurodac Regulation—particularly Article 29—which is the *lex specialis*.

In particular, Article 77 of the GDPR prescribes the right of individuals to lodge a complaint with a DPA if they consider that the processing of their personal data infringes that regulation. The national data protection authority should inform the complaining individual about the progress and outcome of the complaint within a reasonable period, including the possibility of a judicial remedy.[77] Indeed, the role of national DPAs in supervising the lawfulness of the processing is crucial and an "essential correlate of the rule of law."[78] It is all the more necessary in the case of Eurodac, which processes a special category of personal data—fingerprints—collected from a particularly vulnerable group of individuals.[79] The model opted for in the recast Eurodac Regulation—and all other EU centralized information systems, for that matter—consists of two independent tiers of external supervision.[80] On the one hand, the monitoring of the national authorities is entrusted to national DPAs.[81] On the other hand, the supervision of EU institutions, *in casu* eu-LISA, is bestowed on the European Data Protection Supervisor (EDPS).[82] The latter shall ensure that an audit of eu-LISA's personal data processing activities is carried out at least every three years; a corresponding report should reach the European Parliament, Council, the Commission, eu-LISA, and the national data protection authorities.[83] Internally, eu-LISA is further supervised by its Data Protection Officer, who receives complaints concerning actions of eu-LISA affecting individuals.[84] As foreseen in Article 32 of the recast Eurodac Regulation, the two branches meet in the framework of the Eurodac Supervision Coordination Group, which

[75]As mentioned above, refugee status is national. For recognition rates, see *Asylum Recognition Rates in the EU/EFTA by Country, 2008–2017*, Migration Policy Inst., https://www.migrationpolicy.org/programs/data-hub/charts/asylum-recognition-rates-euefta-country-2008-2017 (last visited Feb. 27, 2021).

[76]*See* Directive 95/46 of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 28, 1995 O.J. (L 281) 31 (EC).

[77]*See* GDPR, *supra* note 69, at art. 77(2).

[78]*See* Nikolaus Marsch, *Networks of Supervisory Bodies for Information Management in the European Administrative Union*, 20 Eur. Pub. L. 127 (2014).

[79]*See* Eurodac Supervision Coordination Group, *Activity Report 2016–2017*, at 3 (2018), https://edps.europa.eu/sites/edp/files/publication/19-01-07_eurodac_supervision_coordination_group_activity_report_2016-2017_en.pdf.

[80]Marsch understands this approach as vertical centralization. *See* Marsch, *supra* note 78, at 143. *See also* Franziska Boehm, Information Sharing and Data Protection in the Area of Freedom, Security and Justice – Towards Harmonised Data Protection Principles for Information Exchange at EU-Level 395 (2013).

[81]*See* Recast Eurodac Regulation, *supra* note 10, at art. 30.

[82]*See id.* at art. 31.

[83]*See id.* at art. 31(2).

[84]*See* eu-LISA Regulation, *supra* note 35, at art. 18(2)(a).

https://doi.org/10.1017/glj.2021.11 Published online by Cambridge University Press

comprises national DPAs and the EDPS and, thus, exemplifies vertical cooperation between national supervisory authorities and the EDPS.[85]

Articles 29(14) and (15) of the recast Eurodac Regulation particularize the protection of Article 77 of the GDPR—guaranteeing the right to bring a complaint before competent authorities—in two cases: a) If asylum seekers are refused the right of access, or b) in order to exercise their rights of correction or deletion. These rights—access, correction, and erasure—along with the right to information,[86] constitute the key individual rights foreseen in data protection law and are enshrined in the recast Eurodac Regulation.[87] Individual rights derive from the right to good administration, a general principle of EU law that binds EU institutions and bodies—as well as Member States—in all procedures, including procedures for granting protection.[88] They are also in line with the principle of transparency, as enshrined in Article 5(1) of the GDPR.[89] In fact, the individual rights of access and correction are also foreseen in Article 8 of the Charter. Particularly, the right to access is an integral part of the right to an effective remedy, as protected under Article 13 of the European Convention on Human Rights (ECHR) and Article 47 of the Charter. The European Court of Human Rights (ECtHR) has found that a person needs to be able to challenge the data storage or to refute the truth of the information, including when it is stored for security purposes.[90] In addition to these individual rights, the recast Eurodac Regulation provides that any person who has suffered damage as a result of an unlawful processing operation or any act incompatible with the recast Eurodac Regulation is entitled to receive compensation from the Member State responsible for the damage suffered.[91] Claims of compensation against a Member State shall be governed by the provisions of national law of the defendant Member State.

Despite the existence of extrajudicial remedies, as outlined above, their effectiveness is highly questionable. First, national DPAs may receive complaints related to the rights of access, correction, and deletion, but not in connection with how applicants are informed about the purposes and processing of their personal data within Eurodac—where, as shown later in this section, there are practical implementation problems with asylum seekers not always receiving and/or comprehending the necessary information during fingerprinting. Second, though available information is scarce, practice shows that recourse to DPAs is very limited. The Eurodac Supervision Coordination Group reports that in the period from 2016–2017, the DPAs in only two participating States—Ireland[92] and the UK[93]—received complaints.[94] In the 2014–2015 reporting period, Denmark was the sole Member State that received two complaints; but the Danish authorities were unable to get in touch with the applicants, who departed Denmark shortly after filing the complaints.[95] Though the primary focus of this Article is on horizontal cooperation, it is worth noting that the EDPS—who, as aforementioned, may receive complaints concerning the

[85]*See* Marsch, *supra* note 78, at 142–43.

[86]*See* Recast Eurodac Regulation, *supra* note 10, at arts. 29(1), 29(2), 29(3).

[87]Reference is made to Article 12 of Directive 95/46, *supra* note 76, which has been replaced by the GDPR.

[88]ECJ, Case C-604/12, H.N. v. Minister for Justice, Equality and Law Reform and Others, ECLI:EU:C:2014:302 (May 8, 2014), para. 50, http://curia.europa.eu/juris/liste.jsf?num=C-604/12.

[89]The rights are also foreseen in the GDPR. *See* GDPR, *supra* note 69, at arts. 15–17.

[90]Rotaru v. Romania, 2000 V Eur. Ct. H.R. 192, para. 72, http://hudoc.echr.coe.int/eng?i=001-58586.

[91]*See* Recast Eurodac Regulation, *supra* note 10, at art. 37(1).

[92]The cases are analyzed below because—though they involve Eurodac—technically, they relate to information exchange following the procedure prescribed in Article 34 of the Dublin III Regulation. *See infra* Section D.

[93]The case involved the deletion of data. The extremely low number is in striking contrast with the finding that deletion is not done routinely, because the Member State that inserted the data is not aware of the change of status. *See* Eurodac Supervision Coordination Group, *Coordinated Inspection Report on Advance Deletion of Data* (Dec. 2011), https://edps.europa.eu/sites/edp/files/publication/11-12-09_eurodac_report_en.pdf.

[94]*See Activity Report 2016–2017*, *supra* note 78, at 15, 22.

[95]*See* Eurodac Supervision Coordination Group, *Activity Report 2014–2015*, at 9 (2016), https://edps.europa.eu/sites/edp/files/publication/17-03-14_eurodac_supervision_coordination_group_activity_report_2014-2015_en.pdf.

https://doi.org/10.1017/glj.2021.11 Published online by Cambridge University Press

management of Eurodac by eu-LISA—has also received no complaint during these reporting periods. Prior to 2016, there is no available information.[96]

The few complaints before national DPAs go hand in hand with the limited number of requests for the exercise of individual rights before national authorities. The great majority of Member States have not recorded any requests for access since July 2016. One Member State recorded six requests in 2016, fifty-five requests in 2017, and twenty requests in early 2018. Several Member States have records of two requests, and one has reported less than five.[97] According to eu-LISA, in 2015, eighty-nine requests for access were submitted. In 2016, the number rose to 156.[98] Only two Member States have received one request from a data subject to correct his or her personal data.[99] In light of the above, it cannot be reasonably expected that asylum seekers lodge complaints with national DPAs. If the exercise of their individual rights of access, correction, or deletion—which are prerequisites for a complaint—is very limited, how can they have recourse to the DPAs? The fish stinks from the head down.

The disappointing landscape may be attributed to three main reasons. First, asylum seekers may be prevented from lodging requests and complaints due to administrative obstacles and language barriers. In the case of asylum seekers, such hurdles may involve their persecution or conflict in their country of origin. For example, FRA refers to the case of an asylum seeker in Sweden who was not in a position to present a Syrian passport, which she had been requested to present as proof in order to carry out a correction.[100]

Second, the provision of information to applicants about the purposes of Eurodac and their individual rights presents problems. Officers find it challenging to give information on all aspects of the data processing at the time of taking fingerprints. The right to information—pursuant to the recast Eurodac Regulation—includes the provision of information regarding the rights of access, correction, and deletion, as well as the right to receive information on the procedures for exercising those rights—including the contact details of the controller and the national supervisory authorities.[101] This results in people often being unaware of why they give their fingerprints and what happens to them. In that respect, the Eurodac Supervision Coordination Group notes that national authorities try to verify that asylum applicants are being asked to confirm whether they have understood the information with which they have been supplied.[102] However, some Member States do not use the model leaflets, in accordance with Article 29(3) of the recast Eurodac Regulation.[103] Although understanding the administrative procedures may be a common issue in relation to all information systems, asylum seekers face additional challenges. They may not be able to absorb data protection-related information as they may be preoccupied with more acute priorities—primarily, the need for protection.[104]

Third, it is not just asylum applicants who may lack awareness. The limited pool of specialized lawyers and NGOs with expert knowledge on biometrics and data protection rules also plays a role. Legal professionals interviewed by FRA note the rarity of such cases coupled with the length of the process and the lack of available expertise in technical matters. However, a question

[96]There are activity reports, but they do not detail the lodging of complaints.

[97]*See* Eurodac Supervision Coordination Group, *Report on the Exercise of Data Subjects' Rights in Relation to Eurodac*, at 9 (Nov. 2019), https://edps.europa.eu/sites/edp/files/publication/2019_11_eurodac_report_data_subjects_rights_en.pdf.

[98]*See* European Union Agency for Fundamental Rights, *supra* note 72, at 100–01.

[99]*Id.*

[100]*See Id.* at 101.

[101]*See* Recast Eurodac Regulation, *supra* note 10, at art. 29(1)(e).

[102]Nevertheless, a minority of Member States assume that the applicants have understood. *See Report on the Exercise of Data Subjects' Rights in Relation to Eurodac*, *supra* note 97, at 5.

[103]*Id.* at 6–7. It is noteworthy that the 2016 proposal for a recast Eurodac Regulation has strengthened the right of information. Article 30, as negotiated, prescribes that more extensive information will be provided in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. *See* Recast Eurodac Regulation, *supra* note 10, at art. 30. Additional safeguards are included in relation to minors.

[104]*See* European Union Agency for Fundamental Rights, *supra* note 72, at 101.

https://doi.org/10.1017/glj.2021.11 Published online by Cambridge University Press

emerges: Are the cases rare because there are no specialized legal professionals, or will the number of cases remain low even if there is expertise?[105] One can only speculate, but as awareness of the use of personal data by applicants grows and as more trained professionals become available for legal representation, the more likely it is that the "tools" offered by data protection legislation will be effectively used. Furthermore, if the more pressing needs for humane living conditions of asylum applicants are safeguarded, the more likely it is that they will consider other matters encroaching upon the protection of their fundamental rights, such as the processing of their personal data.

IV. Judicial Remedies: In-Between Limited Review and Interstate Trust

Lodging a complaint before a national supervisory authority is not an "effective remedy," according to Article 47 of the Charter, as the intervention of a "tribunal" is necessary. The GDPR, as the *lex generalis*, confirms that the right to an effective judicial remedy must be provided in relation to decisions by the "controller" or the "processor" of personal data[106]—that is, the Member State(s) processing Eurodac data—as well as the supervisory authority.[107] Furthermore, apart from governing extrajudicial remedies, Articles 29(14) and (15) of the recast Eurodac Regulation ensure the right to an effective judicial remedy by guaranteeing the right to bring an action before the courts of the State in the same cases that were mentioned in the previous section: If individuals—whose data is processed in the system—are refused the right of access, or in order to exercise their rights of correction or deletion.

Legal scholars correctly point out that the traditional national system of judicial review is challenged in the case of cross-border composite procedures,[108] like Eurodac, primarily because the final administrative act under review is the result of the input of administrative actors of different Member States.[109] In addition, the factors listed in the previous section—affecting recourse to extrajudicial remedies—may equally affect judicial review. The paragraphs below elucidate examples of relevant case law by distinguishing between cases that dispute the accuracy of the Eurodac record and cases contesting the procedural aspects of Eurodac.

1. Disputing the Eurodac Record

In the early days of Eurodac cooperation, the reliability of a Eurodac match was disputed in two Tribunal cases in the UK. In *YI*, the Immigration Tribunal was asked to rule on how a Eurodac hit should be approached and assessed by an Immigration Judge, in a case where the matched data involved an asylum claim made in Italy at a time when the applicant in question claimed to have been undertaking military service in Eritrea from which he deserted.[110] Whereas the UK Home Office emphasized the sufficient reliability of fingerprint data, the Tribunal opined that the Immigration Judge was right in requiring as evidence more than a mere assertion of a match to prove that the fingerprint records established that the applicant had lodged a previous application in Italy. Thus, specific evidence is required, such as photographs, age, name, and claim details. Though the Tribunal did not contest the correctness of the Italian entry and refrained from commenting on the possibility of a false hit, it did opine that further evidence to confirm the existence of a match is needed. General evidence might also be properly admitted about the

[105] *Id.* at 102.

[106] *See* GDPR, *supra* note 69, at art. 79.

[107] *See id.* at art. 78.

[108] Alexander H. Türk, *Judicial Review of Integrated Administration in the EU*, *in* LEGAL CHALLENGES IN EU ADMINISTRATIVE LAW, *supra* note 3, at 218–56.

[109] *See* Lottini, *supra* note 2, at 135.

[110] *See* YI (Previous Claims, Fingerprint Match, Eurodac) [2007] UKAIT 54, https://tribunalsdecisions.service.gov.uk/utiac/37873.

https://doi.org/10.1017/glj.2021.11 Published online by Cambridge University Press

reliability of the Eurodac system and how it operates.[111] Crucial in the judgment was the fact that the fingerprint match was asserted via an email, with no further information and following a previous unsuccessful attempt.[112] The later case of *RZ* demonstrated that where more evidence is provided, it is extremely difficult to challenge the accuracy of the fingerprint evidence.[113] That case confirmed that fingerprint evidence may be challenged but rejected the claimant's argument that a fingerprint match should be treated as an allegation of fraud, which would engage a higher standard of proof than the balance of probabilities. This finding contradicts the decision in *YI*, where it was opined that the standard of proof is the "proof to a high degree of probability" because the UK Home Office—in essence—accused the applicant of committing fraud.[114] Here, the fact that an identified match was validated through visual inspection by a fingerprint expert was key in finding that the Eurodac match was determinative.

The extent to which Eurodac records are wholly reliable has also emerged in France. In 2016, a Dublin transfer on the basis of a Eurodac match was disputed before the Administrative Tribunal of Nantes. The case involved a Cameroonian who, after having been subject to an expulsion order from Spain for having entered irregularly, applied for international protection in France.[115] The prefecture of Vendée ordered the transfer of the applicant to Spain, which had accepted the "take back" request. The Tribunal found that the prefecture had justified the transfer decision based on the applicant's fingerprints being recorded in Eurodac, which established that he had previously filed an application for asylum in Spain. However, other documents in the file—including an interview carried out by the Spanish authorities—showed that he had in fact been apprehended for an irregular border crossing and had not filed an asylum claim in Spain. Therefore, the transfer decision was based on erroneous information and was thus quashed—also because the applicant's personal circumstances were not examined. The wrongful categorization of the applicant's situation as an asylum applicant, instead of an irregular entrant, had significant implications on the Dublin transfer as—pursuant to Dublin rules—the responsibility for examining the application for international protection ceases twelve months after the date on which the irregular border crossing took place.[116] In this case, the French court did not hesitate to expressly review the lawfulness of the applicant's Eurodac registration by the Spanish authorities as an asylum seeker where he was, in fact, an irregular migrant. As the French authorities based their administrative decision to transfer on the mistaken categorization of the applicant by the Spanish authorities, the decision was ultimately challenged and annulled. By reviewing the Eurodac entry, the French court was able to quash the transfer decision.

In the Netherlands, on September 1, 2016, the Dutch Council of State (*Raad van State*) ruled on the declaration of an asylum application as inadmissible by the State Secretary and corresponding refusal to grant a temporary residence permit.[117] It did so because the asylum seeker in question already enjoyed international protection in Greece, as per the corresponding Eurodac record dated from January 2015.[118] However, the Eurodac search dated back to September 2015 and, as a result,

[111]*Id.* at para. 15.

[112]*Id.* at para. 16.

[113]*See* RZ (Eurodac, Fingerprint Match, Admissible) [2008] UKAIT 7, https://tribunalsdecisions.service.gov.uk/utiac/37822.

[114]This is because the UK Home Office, in essence, asserts that the applicants committed fraud. *See* R v. Sec'y of State for the Home Dep't ex parte Khawaja [1982] UKHL 5, [1984] 1 AC 74 (appeal taken from Eng.). *See also RZ*, *supra* note 113, at para. 12.

[115]Tribunal Administratif de Nantes [TA Nantes] [Nantes Administrative Court], Feb. 18, 2016, 1600829, https://www.asylumlawdatabase.eu/sites/default/files/aldfiles/TA%20Nantes%20-%2018022016%20-%20defaut%20examen%20%28Dublin%20Espagne%29%20-%20copie%202_0.pdf (Fr.).

[116]*See* Dublin III Regulation, *supra* note 9, at art. 13(1).

[117]ABRvS 1 september 2016, ECLI:NL:RVS:2016:2441, *Raad van State*, 201604335/1/V3, *available at* https://www.raadvanstate.nl/@105053/201604335-1-v3/ (Neth.).

[118]Beneficiaries of international protection have their record marked in Eurodac. *See* Recast Eurodac Regulation, *supra* note 10, at art. 18.

https://doi.org/10.1017/glj.2021.11 Published online by Cambridge University Press

the information extracted was not sufficiently recent when the case was heard in May 2016. The Council of State confirmed that the State Secretary may, in principle, rely on information from another Member State and only has a duty to verify the information under certain circumstances.[119] As the Greek authorities were obliged under Article 18(3) of the recast Eurodac Regulation to remove a Eurodac result when the status stated therein had been revoked and/or the foreign national had not substantiated that the Eurodac result was incorrect in his case, according to the Court, there were no such circumstances. Thus, the State Secretary was allowed to rely on the Eurodac result without further investigating the residence status of the foreign national in Greece. However, the Court contended that the time had elapsed because the search in Eurodac by the Dutch authorities should be minimal and that information needed to specify the residence rights of the applicant upon return. Lacking these elements, the Council of State ruled that the State Secretary was required to further investigate whether the applicant was still in possession of a valid residence permit or any other permission to reside, issued by the Member State in question. This is because Article 18(3) does not prescribe specific time limits for national authorities to update the relevant records in cases when the circumstances of an applicant have changed. Therefore, it could not be assumed that the information was updated. As a result, the presumption that the applicant would be granted a residence permit or any other form of permission to stay upon return to Greece was unjustified. The reasoning of the Dutch Council of State was based on the lacuna in the prescriptions of the recast Eurodac Regulation and must be interpreted as inserting an asterisk to the trustworthiness of data from other Member States. Although in principle there is interstate trust, the time elapsed since the check of the Eurodac record is crucial. Though the Council of State did not explicitly review the Eurodac record by the Greek authorities, as in the previous case, it did implicitly express doubts as to its accuracy and reliability. Accordingly, the Council of State referred the case back to the State of Secretary, mandating further investigation and requiring the administration to complete a more thorough investigation of individual cases.

More recently, in October 2019, the District Court of 's-Hertogenbosch released an interim judgment[120] in a case involving a Ghanaian national who disputed the Eurodac hit—which was triggered due to prior lodging of claims in Italy and Switzerland—alleging, *inter alia*, that he had traveled through France. On the basis of the hit, his asylum application was not processed and a "take back" request had been accepted by the Italian authorities. The court was requested to impose an interim measure against the decision rejecting the asylum application and to allow the conduct of a counter-expertise investigation, which was originally denied by the Secretary of State. The Court disagreed on the basis of the principle of equality of arms,[121] opining that the applicant should be allowed to provide evidence to the contrary. The decision was based on a close reading of Article 22(3) of the Dublin III Regulation—in connection with Annex II, List A of Commission Implementing Regulation 118/2014[122]—according to which a "take back" request is supported by

[119]*See* ABRvS 12 augustus 2014, ECLI:NL:RVS:2014:3127, *Raad van State*, 201304293/1/V4, *available at* https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RVS:2014:3127 (Neth.). This case concerned the return of an irregular migrant who held a residence permit in another Member State and the extent to which the State Secretary ought to further investigate the validity of that permit.

[120]Rb. Den Haag 10 december 2019, *Rb Den Haag*, NL19.24439, JV 2020/59, ve19003512, *available at* https://jure.nl/ECLI:NL:RBDHA:2019:13122 (Neth.).

[121]The Court referred to case law of the ECtHR on Article 6 ECHR. It acknowledged that in *Maaouia v. France*, the ECtHR determined that Article 6 of the ECHR does not apply to procedures regarding the entry, stay, and deportation of foreign nationals. Nevertheless, the Court refered to the decisions of the Administrative Jurisdiction Division of the Council of State, which emphasized the importance of the right to equal opportunities and the right to a contradictory procedure within the legal order, also separate from Article 6 of the ECHR. *See* ABRvS 19 april 2012, ECLI:NL:RVS:2012:BW4915, AR 2012, 282 m.nt. AMM, *available at* https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RVS:2012:BW4915 (Neth.); ABRvS 30 juni 2017, ECLI:NL:RVS:2017:1674, AB 2017, 365 m.nt. LMK en AMLJ, *available at* https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RVS:2017:1674 (Neth.).

[122]*See* KINDT, *supra* note 62.

https://doi.org/10.1017/glj.2021.11 Published online by Cambridge University Press

proof or circumstantial evidence. Proof, which—as aforementioned—includes a Eurodac hit, is relevant "as long as there is not evidence to the contrary."[123] From this, it was inferred that when using Eurodac, a third-country national must be able to provide evidence to the contrary and must be "allowed and enabled" to provide this through counter-expertise. Though the Court acknowledged that the Secretary of State may, in principle, rely on Eurodac data—under the assumption that the manner in which this registration was made has been careful—in the present case, the documents submitted by the applicant had not been examined at all and his statements had been discarded. As a result, based on the argument of "equality of arms," the Court concluded that the applicant should be allowed to provide "evidence to the contrary" and forbade the State Secretary to transfer the person concerned to Italy—as long as the outcome of that investigation was unknown. Though the national court did not review the Eurodac record itself, it instructed the administration to investigate the matter without blindly trusting the information contained in the database. However, as Brouwer submits, it is unclear why the court did not directly refer to the right to effective remedies, which combines the safeguards of Articles 6 and 13 of the ECHR.[124] Based on that right, in *Ghezelbash*—which is discussed in detail below—the CJEU opined that the right of an asylum seeker encompasses the right to appeal against incorrect application of the Dublin criteria in a transfer decision.[125]

Overall, the aforementioned judgments demonstrate the tension between trust in modern technologies and administrative procedures—fingerprint registration in Eurodac—taken place in other Member States, which may not be infallible, and the need to safeguard the fundamental rights of asylum seekers—particularly their right to an effective remedy. The existence of interstate trust at the administrative level is coupled with gaps in effective protection. As Eliantonio has pointed out, national courts are, in principle, competent to review only the acts emanating from the authorities falling within their jurisdiction.[126] As a result, national courts are not allowed to review the legality of measures issued by foreign national authorities. That said, the French case could be interpreted as an example of a national court directly reviewing the legality of the Spanish administrative act of inserting the record in Eurodac. In the other cases from the UK and the Netherlands, though, the courts are silent about the reviewability of the foreign acts. They provided guidance to the administrative authorities on how to treat Eurodac matches and circumscribed the degree of technology-based interstate trust, by noting the need for further evidence to corroborate a match and requiring the delivery of prompt administration. However, the gap in judicial protection remains, with the only available remedy being prescribed in Article 37 of the recast Eurodac Regulation—which foresees a compensatory remedy, on the basis of which Member States are liable for damages caused as a result of an unlawful processing operation or any act incompatible with the regulation.

These findings, in connection with Eurodac, are not an isolated phenomenon. Brouwer,[127] Tidghi,[128] and Eliantonio[129] have highlighted the limited reviewability of information provision measures in the framework of SIS, which registers *inter alia* alerts on unwelcome third-country

[123]*See* Dublin III Regulation, *supra* note 9, at art. 22(3)(a)(i).

[124]Evelien Brouwer, Case Note: Annotatie Rb Den Haag 10 december 2019 , NL19.24439: Eurodac en het recht op contra-expertise (Jurisprudentie vreemdelingenrecht 2020).

[125]*See* ECJ, Case C-63/15, Mehrdad Ghezelbash v. Staatssecretaris van Veiligheid en Justitie, ECLI:EU:C:2016:409 (June 7, 2016), http://curia.europa.eu/juris/liste.jsf?num=C-63/15. For further analysis, see Subsection D(II).

[126]*See* Mariolina Eliantonio, *Information Exchange in European Administrative Law – A Threat to Effective Judicial Protection*, 23 Maastrict J. Eur. Comp. L. 531, 536–37 (2016).

[127]*See* Evelien Brouwer, Digital Borders and Real Rights – Effective Remedies for Third-Country Nationals in the Schengen Information Systems (2008).

[128]*See* Morgane Tidghi, Networks of Information in the European Union: Multi-Level Administrative Cooperation in Composite Decision-Making Procedures 124 (2013).

[129]*See* Eliantonio, *supra* note 126, at 542.

https://doi.org/10.1017/glj.2021.11 Published online by Cambridge University Press

nationals in accordance with Regulation 2018/1861.[130] As in Eurodac, the alleged unlawfulness of an SIS alert resulting in the annulment of the national decision of refusal of entry or stay on national territory has been scarcely reviewed, with the decision in *Forabosco* by the French Court of State being pivotal in this context.[131] However, there is no legal certainty that national courts will directly review possible irregularities of records in EU information systems. Further research on the reviewability of foreign acts is needed in that regard.

One final remark is due here. Although no judgment employs data protection principles per se, the judgments hint towards the importance of the data protection law principle of data quality, which—according to the GDPR—requires the data to be accurate, relevant, and up-to-date.[132] Beyond its data protection origins, the quality of data is linked to the "duty of care" owed by national administrations. In light of the rule of law, safeguarding the administration's ability to rely on accurate data to make decisions that produce legal effects is crucial for the legitimacy of administrative output.[133] Therefore, an in-depth assessment of the information by the administration is necessary.[134] Thus, the case analyzed just above illustrates that interstate trust may clash and prevail over the requirements of the "duty of care," with significant fundamental rights implications. In such cases, enabling the individual to provide counter-evidence and facilitating further investigation—in particular, by providing the applicant with the necessary financial means for further investigation—should be brought within the remit of the "duty of care." Finally, the possibility of asylum seekers to exploit such procedures, so as to overturn transfer decisions and delay the Dublin procedure, cannot be overruled. However, a way forward could be through the use of national procedural rules—for example, as regards the payment of judicial costs.

2. Breaches of the Eurodac Procedure at the National Level

The procedural rules of Eurodac have also been contested before French courts. In certain cases, the applicants sought annulment of their transfer under Dublin rules due to the failure of the French administration to provide applicants with relevant information at the time of fingerprinting, in accordance with Article 29 of the recast Eurodac Regulation and Article 4 of the Dublin III Regulation. On May 10, 2017, the Council of State highlighted that the right is important for the protection of the applicant's personal data in the exercise of the rights of rectification or erasure. However, that is the sole purpose of those rights and such irregularities cannot result in a transfer decision being annulled.[135] Furthermore, according to the Administrative Tribunal of Nantes—in its decision of May 22, 2014—that result could only be achieved when a breach of the right to information was coupled with concerns as to the deteriorated reception conditions in Italy, as a result of the increase of arrivals. In fact, the Italian authorities had not responded to the transfer request.[136] Though these cases do not unearth challenges raised by the multilevel operationalization of Eurodac as a horizontal composite procedure, they nonetheless illustrate that there are significant loopholes in the protection of individual rights of asylum seekers and their recourse to effective remedies—not only at an extrajudicial level, as stressed earlier, but also at a judicial level. A way forward could be the assignment of specific consequences in cases of breaches of individual rights at a national level, in a future recast of the Eurodac rules.

[130]Regulation 2018/1861, *supra* note 33.

[131]CE Ass., June 9, 1999, 190384 (Fr.).

[132]*See* GDPR, *supra* note 69, at art. 5(1)(c).

[133]*See* Hofmann & Tidghi, *supra* note 4, at 150.

[134]*Id.*

[135]CE Ass., May 10, 2017, Rec. Lebon 510, Éé https://www.asylumlawdatabase.eu/sites/default/files/aldfiles/France%20-%20Le%20Conseil%20d%27État%20_%20Décision%20406122.pdf (Fr.).

[136]Tribunal Administratif de Nantes [TA Nantes] [Nantes Administrative Court], June 22, 2015, 1505089, https://www.asylumlawdatabase.eu/sites/default/files/aldfiles/France%20-%20Tribunal%20Adminnistratif%201505089.pdf (Fr.).

https://doi.org/10.1017/glj.2021.11 Published online by Cambridge University Press

Finally, the Administrative Court of Appeal of Lyon was confronted with the case of an Afghan national who submitted an asylum claim in France, but whose fingerprints were recorded in Slovakia, Sweden, and Italy in previous years.[137] As a result, he was issued with a transfer order to Italy, which he contested—not because he questioned the reliability of the matches but due to an infringement of Article 25(4) of the recast Eurodac Regulation regarding the verification of the match by a fingerprint expert. The Court took the view that because the reliability of the information resulting from the comparison is not seriously criticized, that procedural guarantee—even if breached—was not serious enough to invalidate the transfer order. The latter case may be interpreted as the French court showing deference to the Eurodac record, as inserted by the Italian authorities, in an implicit leap of faith in relation to the system and its reliability.

The cases above demonstrate a striking contrast between disputing the Eurodac record and following the procedures. In essence, a violation of the right to information—pursuant to the Eurodac Regulation—may only influence the exercise of individual rights and has no bearing in the Dublin process, thus breaking the inextricable link between Eurodac and Dublin. As for the verification of fingerprints, the judgment reveals that in practice, a violation of Eurodac rules will not affect the transfer process. This interpretation of Article 25(4) is not supported by the text and is *contra legem*. According to Article 25(4), the match must be "immediately checked in the receiving Member State by a fingerprint expert as defined in accordance with its national rules, specifically trained in the types of fingerprint comparisons." Consequently, there is no room for maneuver for national authorities to avoid such verification. Considering the rarity of these cases before courts, this approach of tolerance towards the irregularities by national authorities may increase their appetite to circumvent the verification stage *en masse*, effectively neutralizing the guarantees embedded in the recast Eurodac Regulation.

D. Information Sharing Under the Dublin III Regulation

As mentioned in the introduction—in addition to the Eurodac rules—the Dublin system itself lays down provisions regulating horizontal transnational cooperation among administrations, without the involvement of EU institutions, agencies, or bodies. These rules involve information sharing, both before and after establishing the responsibility of the Member State. In the sections below, these rules are explored, starting with those regulating information exchange with a view to carrying out a transfer.

I. Pre-Dublin Transfer

Article 31(1) of the Dublin III Regulation foresees the possibility for the exchange of "personal data which is appropriate, relevant and non-excessive" to ensure that the competent authorities can provide the person with adequate assistance. Furthermore, Article 32 details rules specifically concerning the sharing of health data requiring the transferring Member State to transmit information on any special needs, which may include information on that person's physical or mental health. Use of health data must only take place between health professionals who receive the health certificates, and the explicit consent of the applicant and/or their representative is necessary.

These provisions were inserted in the latest incarnation of the Dublin Regulation, and the explanatory memorandum shows their clear rationale, namely "ensuring continuity in the protection offered to applicants under the Dublin procedure subject to transfer decisions."[138]

[137]CAA Lyon, Nov. 20, 2018, 18LY01453, https://www.legifrance.gouv.fr/affichJuriAdmin.do?oldAction=rechJuriAdmin&idTexte=CETATEXT000037640709&fastReqId=903002766&fastPos=1 (Fr.).

[138]*See Commission Proposal for a Regulation of the European Parliament and of the Council 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*, at 13, COM (2008) 820 final (Dec. 3, 2008).

https://doi.org/10.1017/glj.2021.11 Published online by Cambridge University Press

As a result, these rules are aimed at increasing the level of fundamental rights protection afforded to asylum seekers. Therefore, their enforceability before national courts as rules aimed at raising the protection of fundamental rights of Dublin transferees cannot be disputed. As in the case of biometric identifiers, health data also constitutes a special category of personal data. Under Article 9(1) of the GDPR, high standards of protection are therefore required. Consequently, the fact that health data may have been accessible to staff members other than health professionals—including the police, thus in violation of the purpose limitation principle of data protection law[139]—could be subject to litigation before national courts.[140] The same applies in cases where health data is transmitted without the consent of the individual.[141]

II. Preliminary Checks Before Establishing Member State Responsibility

Article 34 provides an information exchange mechanism with a view to making a preliminary check as to whether there is a criterion that is likely to determine another State's responsibility for examining an application for international protection.[142] Such requests are submitted through DubliNet, using Annex V of Commission Implementing Regulation 118/2014. This is a useful option in cases where there is only limited circumstantial evidence that another Dublin State is responsible for examining a claim.

Article 34 contains detailed safeguards on the categories of data requested and shared, the authorities involved, and the individual rights of the applicant. In particular, every Member State must communicate to any Member State personal data—to the extent that is appropriate, relevant, and non-excessive—for determining the Member State responsible, examining the application for international protection, and implementing any obligation under the Dublin system.[143] There is an exhaustive list of categories of data to be shared, including personal details of the applicant, identity and travel papers, and Eurodac fingerprints.[144] The applicant must give their consent in writing to the exchange of this information. There is leeway to the requested State to refuse to respond if the communication of such information is likely to harm its essential interests, or the protection of the liberties and fundamental rights of the person concerned or others.[145] Any request for information shall only be sent in the context of an individual application for international protection. Yet, according to Article 34, requests must not be sent without some indication of the basis upon which potential responsibility might be determined. This is to prevent Member States from making an excessive number of purely speculative, blanket requests to each other.[146] As a result, Article 34(4) foresees that the request must detail the "grounds on which it is based" and, where its purpose is to conduct a preliminary check for potential responsibility of the requested Member State, evidence or reference to a specific part of the applicant's statements must be communicated.

[139] *See* GDPR, *supra* note 69, at art. 5(1)(b). The principle requires that data be collected for specified, explicit, and legitimate purposes, and not be further processed in a manner that is incompatible with those purposes.

[140] Some Member States have reported that health data may be brought to the attention of other authorities, such as social welfare and reception officers, legal representatives, police, and immigration services dealing with a particular case. *See* European Commission, *supra* note 65, at 64.

[141] *Id.*

[142] Requests for exchange of information may also take place in some Member States—Norway, Greece, and Denmark—for family tracing purposes. *See* UNITED NATIONS HIGH COMM'R FOR REFUGEES, LEFT IN LIMBO: UNHCR STUDY ON THE IMPLEMENTATION OF THE DUBLIN III REGULATION 104 (2017), https://www.refworld.org/docid/59d5dcb64.html.

[143] *See* Dublin III Regulation, *supra* note 9, at art. 34(1).

[144] *See id.* at art. 34(2).

[145] Communication is subject to prior approval of the applicant; in other words, their consent must be sought as the basis for the lawful transfer of data. *See id.* at art. 34(3).

[146] *See* U.K. Home Office, *Dublin III Regulation*, at 33–34 (Aug. 14, 2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/882400/Dublin-III-regulation-v3.0ext.pdf.

https://doi.org/10.1017/glj.2021.11 Published online by Cambridge University Press

Any exchange of information may take place between authorities designated by the Member States[147] and specific authorities and courts within the receiving Member State.[148] In addition, the forwarded information must be accurate and up-to-date.[149] As in the case of Eurodac, the applicant has the right to be informed upon request of any data concerning them[150] and to seek their correction or deletion.[151] In terms of remedies, the applicant is entitled to bring an action or a complaint before the competent authorities, or courts or tribunals of the Member State which refused the rights of access, correction, or erasure. Finally, the retention period of the transmitted data is determined under national law and must be for so long as it is necessary for the purposes for which they are exchanged.[152]

A first issue emerging from the operationalization of Article 34 concerns the extent to which interstate trust in the procedures and information provided by another Member State extends beyond the prescriptions of the recast Eurodac Regulation to encompass information on the applicant. This information is collected and stored at the domestic level and under national legislation. An insight into the extension of trust beyond the Eurodac requirements may be found in a Dutch case involving an Eritrean asylum seeker who, though a minor, was registered as an adult by the Italian authorities. When she applied for international protection in the Netherlands, she informed the immigration authorities (IND) that she was in fact fifteen. The IND, however, refused to treat her as a minor—relying upon the data submitted by the Italian counterparts on the basis of the principle of interstate trust. As a result, the minor did not receive appropriate protection, even though she corroborated her statement about her age with documents, and her appearance and behavior made clear she was a minor at the time. In its decision of April 4, 2019,[153] the Dutch Council of State affirmed the importance of interstate trust, holding that the State Secretary had—in principle—rightly assumed that the registration of the applicant as an adult had been carried out carefully, so that it was up to the foreign national to demonstrate that the date of birth registered in Italy was incorrect.[154] In the Court's view, the applicant had failed to do so; a baptism document that was submitted was not accepted, as it was not an identifying document issued by the Eritrean authorities. Furthermore, as a copy of a school card did not include her place of birth, that was also considered insufficient.[155] Therefore, the Court found that it was correct not to doubt the date of birth registered in Italy and thus to not offer an age test. This is despite the fact that the incorrect registration of a minor's age is a common occurrence—particularly in periods of chaos, when large numbers of asylum seekers arrive, but sometimes also due to miscommunication or a lack of information provided to minor asylum seekers.[156] The Court accepted the possibility that the registration by the Italian authorities could be unlawful but placed the burden of proof on the applicant, without properly taking into account the surrounding circumstances, such as the possible minority of the applicant or the country involved in the process. Read in conjunction with the Dutch judgments discussed in Subsection C(IV), it can be argued that in order to safeguard the right to an effective remedy, the Council of State could have mandated the minor's age to be further investigated by the

[147] *See* Dublin III Regulation, *supra* note 9, at art. 34(6).

[148] *See id.* at art. 34(7).

[149] *See id.* at art. 34(8).

[150] *See id.* at art. 34(9).

[151] *Id.*

[152] *See id.* at art. 34(11).

[153] *See* ABRvS 11 april 2019, ECLI:NL:RVS:2019:1165, AR 2019, 106, *available at* https://opmaat.sdu.nl/book/SDU_RECHTSPRAAKNL_ECLI_NL_RVS_2019_1165/ECLI_NL_RVS_2019_1165.

[154] *Id.* at para. 6.

[155] *Id.* at para. 6.1.

[156] *See* Evelien Brouwer, *Interoperability and Interstate Trust: A Perilous Combination for Fundamental Rights*, EU IMMIGR. & ASYLUM L. & POL'Y (June 11, 2019), https://eumigrationlawblog.eu/interoperability-and-interstate-trust-a-perilous-combination-for-fundamental-rights/.

https://doi.org/10.1017/glj.2021.11 Published online by Cambridge University Press

IND—for example, through specific medical checks by experts.[157] Otherwise, in the interest of automaticity and trust in information provided by other Member States, the risk of undermining the legal position of asylum seekers is particularly high. The case is thus illustrative of the uneasy relationship between the protection of fundamental rights, including the right to an effective remedy, and interstate trust. It may be argued that this tension is, to some extent, inevitable, as it cannot be expected of the national court to assume jurisdiction and review the lawfulness of the fingerprinting registration in Italy. However, approaching the registration by the Italian authorities with some caution and, in turn, treating the asylum applicant without suspicion of attempting to defraud the authorities could have resulted in a different outcome. There is, of course, the danger that a different approach could allow asylum applicants to exploit the possibility of contesting the fingerprinting process in the receiving country, by claiming irregularities, in an effort to prolong the coming into effect of the transfer decision.

The second issue revolves around the justiciability of the rules enshrined in Article 34, as described above. Some background information is needed here. First, the origins of Article 34 are traced back to Article 15 of the Dublin Convention. Second, Recital 19 and Article 27 of the Dublin III Regulation provide for the right to an effective remedy in respect of decisions regarding transfers "in the form of an appeal or a review, in fact and in law." Third, the article is located under Chapter VII, headed "Administrative cooperation," and in a different chapter of the Dublin III Regulation than Articles 31 and 32, which can be found in Chapter V. The question that emerges is the following: Are the rules of Article 34 merely of an administrative nature, or can they be used by individuals to invoke enforceable rights? In other words, is Article 34 within the scope of Article 27, on the right to an effective remedy? This question was ultimately answered in the negative, in *BS and RS v. Refugee Appeals Tribunal and Ors*,[158] a case concerning two Albanian nationals who lodged an asylum application in Ireland. Due to doubts concerning the circumstances under which they had arrived in the country, the Office of the Refugee Applications Commissioner (ORAC) submitted a request for information to the UK under Article 34 to determine whether that state was responsible for determining their applications in accordance with the Dublin criteria. Due to geographical proximity, it has been found that three-quarters of asylum seekers arrive in Ireland through the UK. That was the case here as well. The UK confirmed that the applicants had been registered with the UK authorities, as they had applied under different names for a visa in Warsaw—information that contradicted the applicants' statements.[159] Thus, in accordance with the Dublin criteria, the UK was responsible for examining their applications, as the country that had issued a valid visa.[160] The problem was that ORAC had failed to provide details of the grounds on which the request was made, as required by Article 34(4). Instead, ORAC transmitted the fingerprints of each applicant to the UK authorities as the indicative evidence. Thus, the applicants claimed that on the basis of the "fruits of the poisoned tree" principle, the information was unlawfully obtained, could not be relied upon, and the transfer orders were unlawful. The Refugee Appeal Tribunal upheld the finding by ORAC that the UK was the responsible Member State, and the applicants sought judicial review.

First, the High Court found that a breach of Article 34 does not give rise to a right to challenge a transfer decision made on the basis of information which may have been retrieved in violation of Article 34.[161] As the title of the article indicates, the rules concern administrative cooperation among Member States.[162] As a result, Article 27 of the Dublin III Regulation—entitling asylum

[157]*See* BROUWER, CASE NOTE, *supra* note 124.

[158]BS and RS v. Refugee Appeals Tribunal and Ors [2016] IEHC 469, para. 22 (Ir.). The judgment cannot be retrieved but the main arguments are quoted in the judgment by the Court of Appeal, which is discussed below.

[159]This data is national. The UK is not a Schengen Member State and therefore the issuance of short-stay visas is subject to national rules.

[160]*See* Dublin III Regulation, *supra* note 9, at art. 12(2).

[161]*See BS and RS*, [2016] IEHC 469.

[162]*Id.*

https://doi.org/10.1017/glj.2021.11 Published online by Cambridge University Press

seekers to a right to an effective remedy, in the form of an appeal or a review in fact and in law against a transfer decision—is not applicable. In support of this view, it was submitted that in her opinions in the cases of *Ghezelbash*[163] and *Karim*,[164] Advocate General Sharpston found that only Articles 7–15 of the Dublin III Regulation—envisaging the hierarchical criteria—could be subject to review and should be included within the remit of a right to an effective remedy.[165] That approach has been endorsed by the CJEU.[166] In Humphreys J's view, the fact that those articles were specifically singled out is a strong suggestion that "other articles of the Regulation are not properly matters for review at the suit of an individual aggrieved applicant."[167] *Ghezelbash* acknowledges a right to an effective remedy in respect of any transfer decision,[168] but not a right of action on the part of an asylum seeker in relation to all aspects of the Dublin III Regulation.[169] Crucially, due to the systematic inclusion of Article 34, the trial judge concluded that a breach of Article 34—by failing to state the grounds of a request—is not an infringement of the rights of the applicant and could merely qualify as an "inconvenience" to the requested Member State, which is not given a more full and complete statement of the reasons why it is sought.[170]

On appeal, it was submitted that Article 27(1) does not specify what components of the decision-making process leading up to the transfer decision may be the subject of an appeal or review.[171] Indeed, Advocate General Sharpston favored a broad interpretation of Article 27(1) that conferred a "wider right of appeal or review, ensuring judicial oversight of the competent authorities' application of the relevant law (including the Chapter III criteria) to the facts presented to them."[172] Thus, there was no barrier in expanding the protection net of the right to an effective remedy beyond Chapter III. Peart J rejected these statements, though he recognized that the Dublin III Regulation contains a variety of procedural and substantive safeguards designed to protect the rights of those seeking international protection. He found that Article 34 "confers no right or entitlement."[173] As a result, it cannot be accepted that the applicants perform a "trick of the loop" to evade transfer when the application of the hierarchical criteria is correct.[174] It is noteworthy that there was a dissenting judgment from Hogan J, who could not "ignore the fact that a good deal of Article 34 appears to be designed to protect the data protection rights of applicants for international asylum."[175] As a result, he took the view that a preliminary reference was necessary, as the question of whether Article 34 gave rise to individually enforceable rights remained open.[176]

The Irish Supreme Court unanimously upheld the Refugee Appeal Tribunal decision and found that there were no issues concerning the applicability of Article 34, which required referral

[163]*See Ghezelbash*, Case C-63/15.

[164]*See* ECJ, Case C-155/15, George Karim v. Migrationsverket, ECLI:EU:C:2016:410 (June 7, 2016), http://curia.europa.eu/juris/liste.jsf?num=C-155/15.

[165]*See* the case cited *supra* note 158, paras. 20–23; *see also* Opinion of Advocate General Sharpston, Case C-63/15, Mehrdad Ghezelbash v. Staatssecretaris van Veiligheid en Justitie (Mar. 17, 2016); Opinion of Advocate General Sharpston, Case C-155/15, George Karim v. Migrationsverket (Mar. 17, 2016).

[166]*See Ghezelbash*, Case C-63/15 at paras. 30–61; the case cited *supra* note 158, paras. 20–23.

[167]*See BS and RS*, [2016] IEHC 469 at para. 21.

[168]*See Ghezelbash*, Case C-63/15 at para. 51.

[169]*See BS and RS*, [2016] IEHC 469 at para. 22.

[170]*Id.* at para. 25.

[171]*See* BS and RS v. Refugee Appeals Tribunal and Ors [2017] IECA 179, para. 30, https://www.casemine.com/judgement/uk/5da048364653d07b2518fd6c (Ir.).

[172]Opinion of Advocate General Sharpston, Case C-63/15, *supra* note 165, at para. 62.

[173]*See BS and RS*, [2017] IECA 179 at para. 47.

[174]*See id.* at para. 48.

[175]*See* BS and RS v. Refugee Appeals Tribunal and Ors [2017] IECA 179, para. 25 (Hogan, J., dissenting), https://www.casemine.com/judgement/uk/5da048364653d07b2518fd6c (Ir.).

[176]*Id.* at paras. 26–28.

https://doi.org/10.1017/glj.2021.11 Published online by Cambridge University Press

to the CJEU.[177] The Court opined that, according to Article 34(2), fingerprints are listed among the information that may be sought by the requested country. The fact that the UK did not ask Ireland for fingerprints did not mean they could not be provided and, as a result, no breach of Article 34 took place.[178]

In light of the above, applicants whose data may have been transferred in breach of Article 34 are not effectively protected, due to the defected systematic categorization within the Dublin III Regulation. As a result, any exchange of items beyond the list of Article 34(2), particularly in cases where they are found responsible for the examination of the application and where they request information about the grounds of the application for international application, is not protected.[179] Similarly, in cases where the applicants are not informed about the transfer of their data—in breach of Article 34(9)—there is no requirement by EU legislation for a remedy, and protection is thus dependent upon the prescriptions of national law, if any. Indeed, the Dublin Evaluation report suggests that in cases of breaches in data protection, the applicants may have recourse to remedies if and in accordance with national legislation—which can take the form of appeals to challenge decisions,[180] or complaints sent to the national authority dealing with data protection or other similar competent authorities.[181] It is thus regrettable that the Irish courts did not consider it appropriate to submit a reference for a preliminary ruling to the CJEU for an interpretation of Article 34. The interpretation by the Irish Supreme Court may render Article 34 devoid of its protection function. In essence, the systemic approach took precedence over the interpretation of the substance, thus depriving Article 34 of its effectiveness. Arguably, this interpretation may have been preferred so as to prevent potential abuses of the right to effective remedies on behalf of asylum seekers who may take advantage of the intricacies of horizontal administrative cooperation, so as to delay the Dublin process. Indeed, such abuses cannot be fully ruled out. That said, this case illustrates that the purpose of Article 34 remains unclear. It is hereby argued that Article 34 should be interpreted as providing certain requirements to Member States when sending requests for further information to other Dublin states, the disregard of which should carry specific consequences. Otherwise, national authorities may submit such requests based on hunches and statistics. They may even send blanket requests to other countries, seeking further information about applicants in the hope that another Member State may be responsible for examining an asylum claim and, thus, try to "wash off" their responsibilities. The Commission proposal for a revised allocation mechanism replicates the rules on information sharing, which continue to be included under the same title.[182] Thus, it is not impossible that similar challenges may arise in the future. The momentum for legislative reform to address this issue could not be more ideal. One option could be the inclusion of a provision in the legislation explicitly declaring the justiciability of the prescriptions of Article 34 and prescribing specific consequences when domestic authorities fail to abide by those rules.

E. Concluding Remarks

This Article aimed at exploring the effectiveness of judicial and extrajudicial avenues for asylum seekers to seek remedies in connection with information cooperation by Dublin states. It was demonstrated that the determination of the responsible Member State may require one or more intertwined sub-procedures that are functional to the adoption of a final decision, which involves

[177] *See* BS and RS v. Refugee Appeals Tribunal and Ors [2019] IESC 032, https://www.casemine.com/judgement/uk/5da02cc04653d058440f99e6 (Ir.).

[178] *Id.* at para. 34.

[179] For such examples, see European Commission, *supra* note 65, at 81.

[180] As in Cyprus, Denmark, Finland, and Slovenia. *See id.* at 82.

[181] As in Austria, Belgium, Czech Republic, Hungary, Latvia, Malta, Poland, Lithuania, Romania, Switzerland, and Norway. *See id.*

[182] *See Proposed Regulation on Asylum and Migration Management*, *supra* note 17, at art. 40.

https://doi.org/10.1017/glj.2021.11 Published online by Cambridge University Press

intensive information sharing. First, this Article focused on the operation of an advanced form of information sharing through an EU-wide centralized information system, namely Eurodac, which constitutes a composite administrative procedure. Galetta has rightly observed that the design of composite procedures at the EU level is geared predominantly towards achieving efficiency and optimal use of resources, but their multijurisdictional nature may diminish the protection of individual rights and possibilities of effective judicial review.[183] Though, on paper, the recast Eurodac Regulation contains detailed rules on administrative remedies, individual rights, and external supervision, practice shows that extrajudicial remedies are rarely used and the lack of recourse to national DPAs seems to be inextricably linked to the low interest in the exercise of individual rights. Furthermore, trust in national administrations seems to be shared by national courts too, whose hands seem to be tied due to the limits in assuming jurisdiction and reviewing the alleged unlawfulness of administrative acts—the insertion of a Eurodac record in the system—by foreign authorities. As a result, one could argue that national courts may have no other option but to show trust in the administrative practices of other Member States and instead impose limits in the practices of their own administrations. The gap in judicial protection for asylum seekers is evident, as in only one case has the national court directly reviewed the irregular registration in Eurodac and thus annulled the transfer decision. Besides, the case law demonstrated that no court referred the applicant to the national courts of the country that had initially registered the applicant as an asylum seeker. Therefore, on the basis of the case law analyzed in this Article, though interstate trust cannot be described as blind, it surely may be short-sighted sometimes. Such trust is expanded beyond the requirements of Eurodac to encompass the collection of information at the national level. Furthermore, the cases discussed in Section D show that although the Dublin system is concerned with the protection of fundamental rights of asylum applicants—at least to some extent—national courts are unwilling to extend the protective net to Article 34. The contrast between the rationales of Article 31 and Article 34 is striking. As a result, the existing remedies appear to be insufficient to meet the needs of asylum seekers. This Article calls for a more thorough investigation of individual cases—both by national administrations and courts—which will ultimately result in better administrative decisions, without the "ankylosis" that may accompany interstate trust and the limitations of judicial review of administrative decisions coming from outside the jurisdiction of the domestic court.

A few final thoughts are due here. The forthcoming interoperability of EU information systems,[184] including Eurodac—namely, the ability to exchange data and to share information so that authorities and competent officials have the information they need, when and where they need it—is bound to further complicate informational cooperation among national authorities. The input of a significantly larger array of national and EU authorities—for example, Europol or the European Border and Coast Guard (EBCG)—will influence decisions on asylum seekers. As a result, it is expected that the exercise of individual rights, and thus recourse to remedies, will be heavily affected.[185] In this dystopian scenario, recourse to vertical cooperation seems a sensible solution and eu-LISA, as the agency responsible for the operational management of information systems, may play a significant role in that respect. One way forward could be the setting up of an

[183]*See* Diana-Urania Galetta, *Public Administration in the Era of Database and Information Exchange Networks: Empowering Administrative Power or Just Better Serving the Citizens?*, 25 EUR. PUB. L. 171, 179 (2019).

[184]Regulation 2019/817 of the European Parliament and of the Council of 20 May 2019 on Establishing a Framework for Interoperability Between EU Information Systems in the Field of Borders and Visa and Amending Regulations 767/2008, 2016/399, 2017/2226, 2018/1240, 2018/1726 and 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, 2019 O.J. (L 135) 27 (EU).

[185]*See* Niovi Vavoula, *Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?*, 26 EUR. PUB. L. 131, 153–54 (2020).

https://doi.org/10.1017/glj.2021.11 Published online by Cambridge University Press

EU complaints mechanism, based on the EBCG model[186] and with the involvement of the EDPS, where individuals affected by information sharing could seek administrative review. Admittedly, this mechanism may not be effective either. One thing is for sure, however, in an era of the omni-presence of information: Questions about how to reconcile effective administrative cooperation and the protection of fundamental rights are bound to preoccupy us.

[186]Regulation 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard, and Amending Regulation 2016/399 of the European Parliament and of the Council and Repealing Regulation 863/2007 of the European Parliament and of the Council, Council Regulation 2007/2004 and Council Decision 2005/267/EC, art. 72, 2016 O.J. (L 251) 1 (EU).

Cite this article: Vavoula N (2021). Information Sharing in the Dublin System: Remedies for Asylum Seekers In-Between Gaps in Judicial Protection and Interstate Trust. *German Law Journal* **22**, 391–415. https://doi.org/10.1017/glj.2021.11