DE GRUYTER
OPEN

The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination

Lehte Roots

Tallinn Law School,
Tallinn University of Technology
Akadeemia tee 3,
Tallinn 12618, Estonia
E-mail: lehte.roots@ttu.ee

Abstract: *The EURODAC Regulation establishes the database of the fingerprints of asylum seekers. In 2015, the new EURODAC Regulation came in force and some basic concepts that were not in the previous regulation have been changed. The article analyzes the responses to the new EURODAC Regulation from UNHCR and the Commission and the threats that this new regulation is creating. This article aims to find out whether the changes introduced in the new EURODAC will bring potential discrimination concerns and whether asylum seekers are treated as potential criminals and therefore causing stigmatization of those groups of people in society. The article gives an overview of the EURODAC database, fingerprinting and biometric systems, and comparison of old and new EURODAC regulation. The full assessment of the application of the regulation can be done after it has been in force for some time.*

Keywords: *asylum seekers, biometric systems, database, Dublin regulation, EU regulation 604/2013, EURODAC, fingerprints*

1. Introduction

EURODAC Regulation establishes an EU asylum fingerprint database. When someone applies for asylum, their fingerprints are transmitted to the EURODAC central system. EURODAC has been operating since 2003. One of the problems identified is that the EU Member States do not follow the regulation as it was meant to.

doi: 10.1515/bjes-2015-0016 Baltic Journal of European Studies
Tallinn University of Technology (ISSN 2228-0588), Vol. 5, No. 2 (19)

Article 1 of the EURODAC Regulation says:

> *A system known as 'Eurodac' is hereby established, the purpose of which shall be to 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 by a third-country national or a stateless person, and otherwise to facilitate the application of Regulation (EU) No 604/2013 under the conditions set out in this Regulation.* (EURODAC, 2013)

The Commission's European Agenda on Migration (EAM), adopted on 13 May 2015, highlights the need to ensure that all Member States comply with their legal obligation to fingerprint under Articles 4(1) and 8(1) of the EURODAC Regulation (Council Regulation (EC) No. 2725/2000 of 11 December 2000; EURODAC, 2013)[1] Until 2015, the EURODAC database could only be used for asylum purposes. The new Regulation (EURODAC, 2013) allows national police forces and Europol to compare fingerprints linked to criminal investigations with those contained in EURODAC. It should be used under strictly controlled circumstances and only for the purpose of the prevention, detection and investigation of serious crimes and terrorism. From 15 July 2015, the new EURODAC Regulation came in force.

Basically, the new regulation changes the primary purpose of EURODAC which was to find out whether the person has applied for asylum in another EU Member State or not.

In its 2009 Impact Assessment, the European Commission stated that national and European instruments already at hand are not efficient enough in cases where information is needed about asylum seekers or people who crossed the EU border illegally.

Also, the United Nations High Commissioner of Refugees (UNHCR) said that the conditions in which law enforcement authorities should be granted access to asylum seekers' fingerprint data must be stricter than just for the purposes of "prevention, detection and investigation of terrorist offences and other serious criminal offences" (UNHCR, 2012).

This article aims to find out whether the changes introduced in the new EURODAC Regulation raise potential discrimination concerns and asylum seekers are treated as potential criminals.

---

[1] The recast EURODAC Regulation (EU) No. 603/2013 will operate as of 20 July 2015. Until then, the current Regulation shall apply.

The new regulation is far more complex than the old one due to the addition of law enforcement access to the database, which has brought a lot of changes to the security and data protection measures; the new regulation is three times longer than the old one. The whole idea to grant law enforcement authorities access to the EURODAC database started with the principles established in the Hague Programme, in particular the aim of maximizing the effectiveness and interoperability of existing databases and the facilitation of law enforcement information exchange between states (Stefanou & Xanthaki, 2008, p. 311). The principle of interoperability can be defined as the ability of large-scale systems to promote exchanging of data and enable the sharing of information. According to the Commission, interoperability is a technical concept rather than a political or legal one. (Stefanou & Xanthaki, 2008, p. 323) This depolitisizing can, however, have severe effects on the protection of human rights because the lines are blurred between databases established for different purposes and effective scrutiny over the issue might be lost (Stefanou & Xanthaki, 2008, p. 324). Additionally, in 2007, JHA Council also stated that to improve security and fight against terrorism, law enforcement authorities should be granted access to the EURODAC database (Impact Assessment, 2009, p. 5).

UNHCR proposed that the database search should be allowed only if there is a specific criminal offence where there is reason to suspect that the offence was committed by an asylum seeker or a third country national who entered the state irregularly (Impact Assessment, 2009, p. 5). The Commission took this into account to a certain extent by providing in Article 20 of the new EURODAC Regulation three conditions to be granted access to the database: necessary for the prevention, detection or investigation of terrorist offences or of other serious criminal cases; necessary in a specific case; and if there are reasonable grounds to believe that comparison will contribute to the prevention, detection or investigation of the crime at hand, in particular where it is suspected that the offender falls under the EURODAC Regulation threshold (Impact Assessment, 2009, p. 5).

First the article explains what EURODAC database is, then the EURODAC Regulation is described, the human rights concerns are introduced, and after the analysis, conclusions are drawn. The article is based mostly on the relevant Commission reports, scientific articles, EU documentation and legislation. This paper will analyze the changes that the new EURODAC Regulation entails and then follow the reasoning behind the Commission's decision to include law enforcement access to the regulation based on its latest proposal and the 2009 Impact Assessment.

2. The EURODAC database

In order to understand the regulation an explanation is needed about how the collection and storage of fingerprints is carried out. The EURODAC biometric system works based on the collection of fingerprints of all ten fingers from all asylum seekers and immigrants at least of age 14 or over (EURODAC Regulation, Arts. 9 & 14). The digitized form of the fingerprints is then submitted by the national authorities to the Central Unit, which stores all previously submitted data (van der Ploeg, 1999, p. 298). Then a search is conducted comparing all previously stored data with the newly submitted data in order to find a match. If a positive hit is found, then it shows which country should be responsible for processing the person's request and the person can be deported to that country. (van der Ploeg, 1999, p. 298) The data on fingerprints can be transferred to any Member State to check which country should be responsible for looking through the third country national's asylum application (Thomas, 2005, p. 393). This is decided according to the Dublin regulation rules.

The data stored in the EURODAC database includes fingerprints, gender, date of fingerprint taking and a reference number by the state providing the information (Council of the European Union, 2013, Arts. 11 & 14). Although the person remains anonymous in the sense that no name or place of residence is included in the database, the reference number allows the supplying state to link the data in the system to a specific person. This is also a reason why under the European Directive on Data Protection, the information stored in EURODAC is considered personal data. (van der Ploeg, 1999, p. 299)

3. Biometric systems and fingerprints

Fingerprints are widely used in biometric systems, because it requires very little effort to copy and scan a person's fingerprint (Thomas, 2005, p. 377). However, biometric characteristics also need to be usable in the sense that they are not easily changed or affected by ageing, illness or behaviour (Kindt, 2013, p. 53). Now, even though fingerprints are very user-friendly, it is difficult to use them in situations where a person has either deliberately or by accident burned off or otherwise mutilated their fingerprints. This leads to another important quality—reliability. As can be seen, fingerprints can be modified and copied which does not make them the most reliable biometric characteristic. (Kindt, 2013, p. 55) However, it has also been stated that using fingerprints in databases provides

relatively good results with error rates of just 0.1 to 2 per cent. The results are even better if all ten fingers are used for the database, as it is in the EURODAC database. (Kindt, 2013, p. 76)

Fingerprints that are inserted in the EURODAC system have biometric characteristics. Biometric characteristics are human characteristics that are universal, persistent and unique. This means that the particular characteristic has to be something that can be found generally in all human beings, it does not change over a certain period of time and it is unique enough to identify a person from another, meaning that there exists a probability that two templates of a characteristic, for example fingerprints, belong to the same person. Usage of biometric characteristics are valuable in fields such as identity control and verification, which have been exemplified by concerns such as terrorism, asylum and migration, identity theft, and identity fraud. One of the reasons behind this is that biometric information can be understood by officials in the same way anywhere in the world and, most importantly, the information is understood by computers, which allows for fast searches in the database of thousands of samples. The reason why biometric systems were adopted for areas such as migration and asylum was simple—comparing biometric characteristics helps to identify or verify a person without having to talk to the person and establish whether the person is telling the truth about his identity. Without proper documents people can present any identity they want and it would be very difficult to prove otherwise. This is especially problematic in the case of asylum seekers and migrants because often they do not possess any documents while entering a new country. The difficulty lies in establishing whether the documents were knowingly destroyed by the asylum seeker, because otherwise he or she would not be eligible for international protection or the person does not have necessary identification since he or she fled his country due to fear of persecution.

EURODAC is a database that uses biometric characteristics to make the asylum proceedings easier and faster. This is necessary to avoid situations where a third country national asks for asylum in one country but then proceeds to another Member State because the first country did not provide the person with protection or the person just did not like the first state he or she entered. Therefore, through a ‘hit or no hit’ basis of fingerprint matches, the EURODAC system identifies where the asylum seeker crossed the external border to the EU and where he or she stayed prior to making an application for asylum. As the database determines which country should be responsible for the person, the sending of an applicant from one country to another without any of them claiming him or her is avoided.

4. The EURODAC Regulation

Council Regulation (EC) No. 2725/2000 of 11 December 2000 concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of the Dublin Convention was applicable until July 2015 when the new EURODAC Regulation had to be implemented by the Member States. The previous regulation recognized that a fingerprint database like EURODAC would greatly help to apply the Dublin Convention (now the Dublin Regulation) and help establish the identity of asylum seekers (Council of the European Union, 2000, recitals 3 & 4). The Regulation also recognizes that the recording and retention of such data infringes upon the right to privacy and data protection, which is why certain safeguards should be put in place (a concrete data retention period, not to retain for longer than necessary, precise rules for transmission of data, etc.) (Council of the European Union, 2000, recitals 7, 8 & 17).

The regulation sets up a central database of asylum seekers' fingerprints, including also the fingerprints of third country nationals who have crossed the border irregularly. EURODAC consists of a Central Unit which is responsible for operating the central database and a means of data transmission between the Member States and the central database (Council of the European Union, 2000, Art. 1). The fingerprints collected for the purpose of the regulation have three categories: all applicants for asylum of at least 14 years of age, all aliens of at least 14 years of age who are apprehended for crossing the border irregularly, and aliens at least 14 years of age found illegally present in a Member State (Council of the European Union, 2000, Arts. 4, 8 & 11). The data retention period depends on the category the data subject belongs to. Asylum seekers' fingerprints are kept in the central database for ten years while aliens who were caught illegally crossing the border have their data recorded in the central database for two years (Council of the European Union, 2000, Arts. 6 & 10). The third category of fingerprints are taken for the sole purpose of checking whether the person has previously lodged an asylum application in another Member State; however, this is subject to certain conditions and the data is not stored in the central database afterwards, it is solely meant for comparison (Council of the European Union, 2000, Art. 11).

Pursuant to the regulation, data is automatically erased when the retention period is over, or in case of asylum seekers when the person acquires citizenship, or in the case of aliens when they acquire a residence permit or citizenship or leave the territory of the Member State (Council of the European Union, 2000, Arts. 6,

7 & 10, Para. 2). If an asylum seeker is recognized as a refugee, then his or her data will be blocked in the central database or erased (Council of the European Union, 2000, Art. 12).

Pursuant to the old regulation, certain data protection safeguards were put in place for the purpose of balancing the public interest and the infringement upon certain human rights. Member States have to ensure that data is taken lawfully, that it is accurate and up to date and the process of transmission is lawful (Council of the European Union, 2000, Art. 13, Para. 1). The European Commission has to ensure that everyone working in the Central Unit are performing according to the rules and comply with all requests (Council of the European Union, 2000, Art. 13, Para. 4). For the purposes of security, unauthorized access to the database is not allowed and if access is allowed it is only to the information asked for, nothing additional (Council of the European Union, 2000, Arts. 14 & 15). Finally, the data subject has the right to information about the whole system, who takes the data and where it goes, the data subject also has the right to correct the data if it is incorrect and a right to effective remedy if it is taken unlawfully (Council of the European Union, 2000, Art. 18).

In its Policy Plan for Asylum, in 2008 the Commission proposed that the new regulation should unblock data of recognized refugees to avoid the situation of refugees asking for asylum in other countries, to make the rules regarding transmission and erasure of data more clarified and to introduce more information in the system. The idea of allowing access to EURODAC by law enforcement authorities was to be left for further examination. (Council of the European Union, 2008a, Art. 8). Now, in 2015, the law enforcement authorities have a right to access the EURODAC system. As mentioned before, this nevertheless raises different questions of supervision of the data usage and problems of centralization of the services.

The first proposal to amend the EURODAC Regulation was also published by the Commission in 2008. The proposal contained corrections regarding the time periods relevant for transmission, storage and erasure of data, and other amendments to make the system more concrete, but law enforcement access was yet to be introduced (Council of the European Union, 2008b, Arts. 3, 5 & 6). The change happened in 2009, when the Commission proposed to allow law enforcement authorities access to the EURODAC database under certain conditions, which meant that the scope of the Regulation would widen considerably. However, during the preliminary discussions with the Council and the Parliament, in order to speed up the renewal of the Common European Asylum System, the Commission left out the law enforcement access point from its next proposal submitted in 2010

(EDPS, 2012, Art. 3). The step was welcomed by many institutions since the issue of granting law enforcement access to such sensitive data was seen as very problematic (EDPS, 2012, Arts. 2–4).

Despite the initial negative response, the growing trend of granting police bodies access to different databases (e.g., Visa Information System) showed hope for the Commission on going through with another try with a proposal similar to the one published in 2009 (Boehm, 2012a, p. 342). In 2012, the Commission published its final proposal on the changes in the EURODAC Regulation thereby replacing the previous 2010 proposal and the law enforcement access clause was re-included.

In its 2009 Impact Assessment, the European Commission put a lot of emphasis on the issue that national and European instruments already at hand are not efficient enough in cases where information is needed about asylum seekers or people who crossed the EU border illegally. The Commission identified that access to other Member States asylum seekers' databases is problematic (Impact Assessment, 2009, Art. 8). The system in place includes:

1) the information exchange system under the Prüm Council Decision stating on a 'hit or no hit' basis whether a Member State has further information about a person in its national database;
2) Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities;
3) Convention on Mutual Assistance in Criminal Matters under which authorities can access criminal and non-criminal databases;
4) Visa Information System (VIS) which provides information about a person and his or her visa data; and
5) Schengen Information System (SIS) which indicates if a person is wanted by a national authority. (Impact Assessment, 2009, Arts. 7–9)

The problem with the Prüm Decision is that not all Member States store asylum seekers' information in their national databases, unless the asylum seekers are convicted criminals, so for the purposes of crime prevention, detection and investigation EURODAC is not efficient (Impact Assessment, 2009, Art. 9).

Information pursuant to the Framework Decision 2006/960/JHA can be requested from a specific Member State if there are reasonable grounds to believe that the Member State has some information, which might be difficult to figure out in the first place (Impact Assessment, 2009, Art. 9). Next, a request based on the rights of the Convention on Mutual Assistance in Criminal Matters is just time consuming because it entails asking information from possibly all Member

States (Impact Assessment, 2009, Art. 10). Finally, regarding the VIS and the SIS, the fingerprints of asylum seekers are in those databases only if the asylum seeker has a visa or is applying for one and in the case of SIS, if he or she is wanted for arrest (Impact Assessment, 2009, Art. 11).

These are the main reasons the Commission sees that the system was insufficient, regarding information about asylum seekers, and the only way the situation can get better is if the EURODAC database is granted wider access. Cross-border crime is considered one of the most serious threats to society and the inefficiency of the system makes it impossible for law enforcement authorities to perform their duties in the prevention, detection and investigation of serious crimes (Impact Assessment, 2009, Art. 13). The Commission pointed out that it was aware that the number of asylum seekers who are involved in terrorist and other serious crimes might be very small, but since the gravity of the crimes is so large and their impact tremendous, this move is adequately justified (Impact Assessment, 2009, Art. 13).

Interestingly, the Commission itself admits that asylum seekers are not the main source of terrorists and criminals, nevertheless it was decided that the access to the EURODAC database of law enforcement authorities is needed. It leads to the strong presumption that asylum seekers are still seen as potential criminals and terrorists, otherwise this access of law enforcement authorities would not be a question at all.

Additionally, the Commission brought out that 13 states which implement the Dublin System keep asylum seekers' fingerprints in general fingerprint databases or special databases and 12 states allow national law enforcement authorities access to databases containing asylum seekers' fingerprints (Impact Assessment, 2009, Art. 7). This demonstrates that police forces regularly use asylum seekers' data in criminal matters (Impact Assessment, 2009, Art. 7). The impact assessment also showed certain statistics on hit rates. In Germany, the hit rate in a national database containing asylum seekers' fingerprints was 40 per cent; 19.4 per cent of crimes in 2006 were committed by non-nationals and 8.5 per cent of non-nationals were asylum seekers. In the Netherlands, the database containing fingerprints of aliens, including asylum seekers, provided a hit rate of 44 per cent. In Austria, 19 per cent of crime suspects were asylum seekers. In the UK, the hit rate on counter terrorism was 7 per cent in a database containing asylum seekers' fingerprints. However, because the systems behind these statistics are so different, the data is not comparable. (Impact Assessment, 2009, Art. 8) It is important to point out that only the statistics of 4 Member States out of 27 (at the time) were presented in the assessment.

Regarding the situation of human rights, the Impact Assessment only touches upon some of the human rights to be affected. The justification concerning data protection is based on the fact that interference is allowed if it is in accordance with the law, necessary in a democratic society, proportionate and sufficiently precise and clear in the scope of discretion it allows authorities (Impact Assessment, 2009, Art. 16). Nevertheless it is not clear how data protection is controlled and regulated, and whether the supervision is enough to protect the vulnerable groups from the abuse of the data.

The Commission points out that data protection in the area of law enforcement is protected under the Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (Council of the European Union, 2013, Art. 33). To comply with data protection principles and measures, access to authorities will be given only on a case-by-case basis, data subjects will have the right to ask for a correction of the data, they will be provided with effective remedies, and there will be supervision over the whole process (Impact Assessment, 2009, Art. 16). With regard to the asylum seekers, they often do not have an idea that they might have this kind of right to ask for the correction of the data. Also, it is not transparent how EU Member States delete the data from the EURODAC and how a person can access the information entered about him or her to the database, without complicated procedure.

The Assessment further mentions the right to asylum and the negative effect it might have if asylum seekers are discouraged from applying for international protection once they know that their information may be given out to police authorities of other Member States from where it could leak out to third countries (Council of the European Union, 2009, Art. 16). This will be safeguarded by adding a clause which prohibits giving out this data to third countries. Based on these considerations, the Commission concludes that the new EURODAC Regulation will be fully compliant with the Charter of Fundamental Rights of the European Union. Nevertheless the full impact assessment was not done.

5. Responses to the reform

The 2012 EURODAC proposal received a lot of critical response from many institutions because widening the objectives of an existing system entails a lot of analysis and specific evidence on its necessity, which the Commission failed to provide by not performing a new impact assessment and following with the conclusions it developed under the 2009 Impact Assessment. As it will be shown, the European Data Protection Supervisor (EDPS) in particular was very critical about the 2009 Impact Assessment and continued to be critical in 2012 stating that the impact assessment had not been convincing and because so many changes had happened during those three years, new considerations applied and a new assessment should have been conducted (EDPS, 2012, p. 5).

A lot of the criticism follows that the reasoning and evidence provided was not convincing and instead of invading more rights, the EU should rather focus on repairing the existing system (Council of the European Union, 2009, p. 5). Emphasizing the shortcomings of existing databases and systems, is not a good method to prove necessity, without analyzing whether other steps could be taken to improve the existing tools are not good enough (Boehm, 2012b, p. 363). First it should be established what the existing databases and institutions are capable of and what could be changed before establishing new access possibilities. Without this evaluation of the existing system and showing that there is a need for a new one, the law enforcement access seems like a premature decision. (Boehm, 2012b, p. 365)

The EDPS has warned that granting access to additional authorities creates an issue where a database initially regarded as proportionate in terms of privacy, data protection and other rights can be seen as disproportionate if its use is expanded (EDPS, 2011, pp. 4–5). There should be clear proof of the necessity to expand a system made for particular purposes (EDPS, 2011, pp. 4–5). The EDPS commented that access for law enforcement might be necessity in case there is a clear link between asylum seekers and terrorist or other serious crimes (EDPS, 2010, Para. 46).

The statistics of four Member States on hit rates that were not all to the point (e.g., Austrian statistics provided a hit rate for suspects but failed to show the statistics on how many convictions were based on the hit rate) and obviously not enough to show that there is a clear link between asylum seekers and serious crimes (EDPS, 2012, p. 20). Furthermore, before establishing whether there is

a link between criminals and asylum seekers, the assumption of asylum seekers being criminals is a discriminatory one (Boehm, 2012b, p. 364).

In general, the EDPS found three main concerns with the EURODAC 2012 proposal.

Firstly, the EDPS pointed out that instead of using impact assessments complementing the 2008 and 2009 Commission proposal, a new Impact Assessment for the 2012 proposal should have been conducted (EDPS, 2012, p. 3). The relevant Impact Assessment on the matter of law enforcement was the one performed in 2009; however, it becomes irrelevant because it lacks a substantial analysis as it does not show the immediate necessity for law enforcement access in the eyes of the EDPS and it is not backed by enough statistical evidence (EDPS, 2012, p. 4). Additionally, the Impact Assessment repeated the fact that existing databases and systems were insufficient and impractical without actually showing that the combined effort of existing instruments was not good enough and could not be improved in any other way (EDPS, 2012, pp. 5–6). It is clear that the Impact Assessment is outdated and a new one should have been conducted for the 2012 proposal.

Secondly, the EDPS pointed out the challenges of the 'function creep' and the principle of purpose limitation. 'Function creep' arises when something created and used for a certain purpose and objective is gradually widened to incorporate other uses. The EDPS reminded the Commission that this trend should not be tolerated since data collected for one purpose should not be used for other purposes just because it can be done; there should be evidence of necessity and proportionality of the action. (EDPS, 2012, p. 7) Lastly, it is of concern that while EURODAC data obtained and transmitted for the purposes of facilitating the Dublin Regulation is protected by the Data Protection Directive, data transmitted for the purposes of law enforcement is protected by the Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters which are different in the protection they offer (Council of the European Union, 2013, recital 39).

The EDPS further stated that the failure to enrol asylum seekers' fingerprints should not end up in a situation where the asylum seeker is rejected or his application refused (EDPS, 2012, p. 17). It was recommended to add a clause stating that the failure to enrol will not change the legal situation of the person and, especially, it will not affect the asylum seekers' situation with regard to granting international protection (EDPS, 2012, p. 17).

The United Nations High Commissioner of Refugees (UNHCR, 2012, p. 9) has also stated that the conditions in which law enforcement authorities should be granted access to asylum seekers' fingerprint data must be stricter than just for the purposes of "prevention, detection and investigation of terrorist offences and other serious criminal offences". UNHCR proposed that the database search should be allowed only if there is a specific criminal offence where there is reason to suspect that the offence was committed by an asylum seeker or a third country national who entered the state irregularly. (UNHCR, 2012, p. 9) The Commission took this into account to a certain extent by providing in Article 20 of the new EURODAC Regulation three conditions to be granted access to the database: necessary for the prevention, detection or investigation of terrorist offences or of other serious criminal cases, necessary in a specific case and if there are reasonable grounds to believe that comparison will contribute to the prevention, detection or investigation of the crime at hand, in particular where it is suspected that the offender falls under the EURODAC Regulation threshold (UNHCR, 2012, p. 9). This is, of course, a big step forward; however, the idea of the suspect being someone falling under the EURODAC Regulation is only one concrete example based on the wording of the Article and this could leave room for law enforcement authorities to get access even if the condition is not present.

UNHCR is also concerned about information on asylum seekers being passed on to countries of origin putting the asylum seekers and their families in a situation of danger (UNHCR, 2013, p. 5). This is safeguarded in the new regulation, accepted in 2013, by prohibiting the dissemination of EURODAC information to third countries. Another concern is the asylum seekers' access to information. It is necessary that everyone giving their fingerprints for EURODAC's purposes should be informed in the language that they understand as to why their fingerprints are taken, for what purposes regarding the Dublin III Regulation, and that the fingerprints may be used for the prevention, detection or investigation of serious offences (UNHCR, 2012, p. 9).

The EDPS, the Meijers Committee and the UNHCR are all concerned that law enforcement access could lead to the stigmatization of asylum seekers (UNHCR, 2012; EDPS, 2010, Para. 47; 2012b, p. 3). Asylum seekers will be more likely to face criminal investigation because their fingerprints are in a large-scale database, accessible for law enforcement authorities to conduct searches (UNHCR, 2012, Art. 10). This increases exposure to asylum seekers and can lead to a situation where third parties misinterpret the situation and subject the asylum seekers to racism and xenophobia by associating them as criminals. Even if the asylum seeker is found to be innocent, this criminal investigation can leave a mark on the person's social status and can hamper his or her integration into a foreign

society (e.g., employment, renting accommodation, etc.). It may also make the asylum seekers suspicious of the asylum system if the persecution they suffered in their country of origin was performed by their police forces (UNHCR, 2012, Art. 10). Furthermore, the EURODAC database is very specific in the groups of data subjects it entails and therefore discrimination can arise by singling these people out for law enforcement scrutiny (UNHCR, 2012, Art. 11; Council of the European Union, 2012, p. 3).

6. The new EURODAC Regulation

The new EURODAC Regulation starts off by listing the purpose of the Regulation, which is still considered to be the assistance of the Dublin Regulation (Council of the European Union, 2013, Art. 1, Para. 1). Additionally, Article 1, Paragraph 2 points out that the Regulation also sets out the conditions for granting law enforcement access. It is not mentioned that the purpose of the database has changed, because in a sense it has not. The data is still collected first and foremost to facilitate the application of the Dublin system and the granting of access to law enforcement authorities should be rather seen as an exception to the purpose limitation principle (EDPS, 2010, p. 7). However, it is still true that the uses of data are widened from what they originally were.

Now, the EURODAC structure has remained relatively the same, just that the Central Database will also include a Business Continuity Plan and System (Council of the European Union, 2013, Art. 3, Para. 1). Each Member State is to have one National Access Point (a system which communicates with the Central Database) which will carry out transmissions and operations (Council of the European Union, 2013, Art. 3, Para. 2). A major change compared to the old regulation is that 'the Agency' (a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice) will be responsible for the operation management of EURODAC (maintenance, technical developments, developing the Business Continuity Plan and System, Impact Assessment) but also for the supervision and security of the exchange of information (Council of the European Union, 2013, Art. 4, Paras. 1 & 2).

To use EURODAC for law enforcement purposes, Member States have to designate and list the authorities who will have the right to request access to the EURODAC data (Council of the European Union, 2013, Art. 5). As a safeguard to establish whether the requests done by designated authorities are lawful, Member States will designate one authority to act as a verifying authority for

such requests (Council of the European Union, 2013, Art. 6). Obviously the verifying authority has to be independent from the authorities requesting access to information to ensure proper safeguards; however, it is still allowed for the verifying to be part of the same organization as the designated authority, it just cannot take orders from the designated authority or be otherwise attached (Council of the European Union, 2013, Art. 6).

In case the verifying authority is not independent and is part of the same organization as the designated authority, the human rights protection concerns and abuse of usage of personal data will arise. Also, it is not guaranteed that mismanagement of the EURODAC system is controlled and reported in a correct manner. In this case, the principle of separation of powers is not followed and real independence between the units is not available, since they are all under the same organization (Boehm & Cole, 2014, pp. 80–81). Independence is definitely better ensured if the verifying authority is in the form of judicial review, another organization or part of another organization.

Regarding the designation of different authorities, it is welcome that the new Regulation also provides for Europol to designate units which will be authorized to request information and units which will verify such requests (Council of the European Union, 2013, Art. 7). However, in this case both of the units definitely will be part of the same organization.

Some important changes in the new Regulation are included in the provisions regarding the collection and comparison of fingerprints. The new Regulation sets out time limits for the collection of fingerprints—within 72 hours from the lodging of an asylum application or 72 hours after the date of apprehension in case of illegal border crossing (Council of the European Union, 2013, Art. 9, Para. 1; Art. 14, Para. 2). This time limit can be extended for another 48 hours in case the fingerprints are unreadable during the first 72 hours, there is a health concern, or if there are technical problems (Council of the European Union, 2013, Art. 9, Para. 2; Art. 14, Para. 5). These requirements do not apply in case of aliens found illegally on the territory of a Member State because for them the measure is optional. There is also a time limit for advanced data erasure, which stipulates that if a person is granted citizenship then the Central System will inform the Member State of origin within 72 hours of the erasure of data (Council of the European Union, 2013, Art. 13, Para. 2). The same 72 hour limit applies to the erasure of data of third-country nationals who crossed the border illegally if they receive a residence permit, leave the Member State or receive citizenship (Council of the European Union, 2013, Art. 16, Paras. 3 & 4).

The time limit for the retention of data in case of asylum seekers remains the same (10 years); however, the retention of data about third-country nationals who crossed the border illegally has been reduced from 2 years to 18 months, which is not a big change but it is a positive step forward (Council of the European Union, 2013, Art. 16, Para. 1; Art. 12 Para. 1). The data of third-country nationals who are found to be illegally present in a Member State will not be recorded in the Central System like the other two categories of data, only the record of the search will be kept for the purpose of data protection monitoring (Council of the European Union, 2013, Art. 17, Para. 4). The old Regulation was stricter in this sense that the fingerprint data and other data should have been erased and the medium used for transmission destroyed after the comparison was done (Council of the European Union, 2000, Art. 11, Para. 5).

The new Regulation also establishes the rules applicable when the asylum seeker receives international protection. The data will be marked accordingly and other Member States that have produced a hit with that data will be notified; however, the data will remain in the system (Council of the European Union, 2013, Art. 18, Para. 1). For law enforcement purposes the data will be available for comparison for three years after the data subject was granted asylum, after three years the data will be blocked (Council of the European Union, 2013, Art. 18, Para. 2).

Of course, the most important part of the new Regulation is the conditions under which law enforcement authorities can access the database. They are established under Articles 20 (for national law enforcement authorities) and 21 (for Europol) of the Regulation. The first Commission proposal to add the law enforcement access clause to the Regulation was criticized a lot because the conditions for national authorities and Europol differed considerably, giving Europol a lot more discretion and power (EDPS, 2010, Para. 50). This was changed and the requirements are now the same under both Articles 20 and 21.

The first requirement is that other databases should be checked beforehand, which include national databases, identification systems of other Member States under Decision 2008/615/JHA if identification is possible and the Visa Information System (EDPS, 2010, Art. 20). The second set of requirements is that comparison should be necessary for the purpose of prevention, detection and investigation of a serious crime (public interest should override other concerns), it concerns a specific case, and the comparison should contribute to the prevention or solving of the crime, which is fulfilled in particular where the offender or victim is suspected to be an asylum seeker or illegal third-country national (EDPS, 2010, Art. 20). Article 21 regarding Europol's access differs

only insofar as no specific databases are mentioned that should be checked beforehand, it is just stated that everything available to Europol should be checked (EDPS, 2010, Art. 21, Para. 1).

These conditions are only the first safeguards for the protection of data. The new Regulation, similarly to the old Regulation, establishes the requirements for the quality of data; in particular that it should be taken lawfully, it should be correct and up to date (EDPS, 2010, Art. 23, Para. 1). In addition, the Agency will need to supervise that fingerprints are processed digitally and transmitted in the correct data format, that technical requirements for transmission are fulfilled and that data is transmitted only electronically (EDPS, 2010, Art. 24). There are also specific rules on the comparison of data, such as the quality, the time limit for carrying out the comparisons (24 hours), etc. (EDPS, 2010, Art. 25).

The supervision of data protection will be carried out by the European Data Protection Supervisor and national Data Protection Authorities, which will cooperate actively with each other (e.g., they shall meet twice a year) (Council of the European Union, 2013, Arts. 30, 31 & 32). More importantly, the supervision of data protection differs in relation to the different purpose for which the data is used. This essentially means that data used for law enforcement purposes is protected by the Framework Decision 2008/977/JHA, whereas data used for the main purpose of facilitating the Dublin Regulation is protected under the Data Protection Directive (Council of the European Union, 2013, Art. 33). This shows that the level of protection afforded to the personal data differs based on what purpose the data is used for at the time.

7. Conclusion

Since July 2015, law enforcement bodies, both national and Union-wide, can request the comparison of fingerprint data for the purpose of preventing, detecting and investigating terrorist offences and other serious crimes. The aim of the article was to find out whether these changes introduced in a new EURODAC arise potential discrimination concerns and whether asylum seekers are treated as potential criminals.

With regard to privacy and data protection concerns, there were many risks involved already with the initial EURODAC system; however, these risks may increase with the involvement of law enforcement authorities. The following

examples show some of the dangers associated with biometric databases like EURODAC.

First of all, biometric data can be prone to misuse due to its unique features and uses. This is especially so with fingerprints which are in their nature dangerous as they are visible to everyone and leave traces behind. Because of this, fingerprints can be easily collected without the data subject even knowing that someone obtained them which can lead to a situation where a person is identified by these characteristics against his or her will (Kindt, 2013, pp. 337–338). However, the situation gets worse if the fingerprints collected without the knowledge of the data subject are used fraudulently. Often the misuse of biometric data is done for the sole purpose of committing a crime and staging the data subject as a perpetrator when in reality the data subject is a victim. If law enforcement bodies have access to large-scale biometric databases of different regular people (not criminals), then the victim will become a suspect and will have to prove that they did not commit the actual crime. (Kindt, 2013, p. 347) In order to avoid this stigmatization and discrimination it is important to follow Article 20 of the Regulation in a very strict manner and the control over the access to the data should be well registered and monitored. A positive development is that the Commission took into account the critiques of its proposal, to a certain extent, by providing in Article 20 of the new EURODAC Regulation three conditions to be granted access to the database: necessary for the prevention, detection or investigation of terrorist offences or of other serious criminal cases, necessary in a specific case and if there are reasonable grounds to believe that comparison will contribute to the prevention, detection or investigation of the crime at hand, in particular where it is suspected that the offender falls under the EURODAC Regulation threshold.

The misuse of biometric data also increases if stored in a centralized database. Such storage poses several privacy and security risks for asylum seekers as these databases are more prone to unlawful access or unauthorized disclosure of the information contained therein (Liu, 2008, p. 49; Kindt, 2013, p. 359). The European Court of Human Rights has stated that if a centralized database is not adequately protected against unauthorized access then there is a violation against the right to respect for private life and centralized units should be secured appropriately against any unlawful access attempts and attacks (Kindt, 2013, p. 360). With law enforcement bodies now having access to such information, the risk of unauthorized access is growing and it is to be seen whether there are enough precautions taken in the form of how access to information can be obtained and with other means to ensure the proper protection of asylum seekers. Obviously, an excessively long period for storing biometric data will

also increase the risk of misuse or sharing of this sensitive information (Farraj, 2010–2011, p. 933). These concerns were also elaborated before and stated by the EDPS. The access for law enforcement might be a necessity, in case there is a clear link between asylum seekers and terrorist or other serious crimes, but these assessments have to be done according to the legislation and the rule of law. Data collected for one purpose should not be used for other purposes just because it can be done; there should be evidence of necessity and proportionality of the action. It seems that this principle is not followed when the EURODAC Regulation was changed.

Finally, there is concern that arises with the EURODAC database when the fingerprints cannot be enrolled. Mutilation that is self-inflicted can be seen more and more among refugees and asylum seekers to escape the identification by biometric characteristics (Pugliese, 2013, p. 571). As the usage of biometric characteristics becomes even more popular, the number of persons ready to harm themselves also increases (Kindt, 2013, p. 252). The issue of mutilation stems from the fact that the information biometric data gives out is not a personal truth; it is only the truth about the body (Aas, 2006, p. 153). Through the EURODAC database one receives only information as to how many times and where the person has crossed a border or entered a country illegally, but there is no personal knowledge about the reasons for these actions (Aas, 2006, p. 153). Biometric data makes no attempt to find out these reasons and this is good in terms of anonymity and not giving out confidential information; however, because it fails to take into consideration the reasons for international protection it may also put the asylum seeker in a difficult situation.

In addition, the problem of mutilation might also increase with allowing access of law enforcement authorities to the database since there will be an aura of distrust towards the EURODAC system among asylum seekers in fear of persecution and stigmatization. Asylum seekers are not discriminated because of the new EURODAC system; nevertheless, there exists high potential treating them as criminals. This is highlighted also in the UNHCR.

Further, an important addition by the Commission to the safeguards is the prohibition of transferring personal data to any third country. Further, if a hit has been obtained by a Member State for law enforcement purposes, then data shall not be transferred to third countries if there is a risk that otherwise the data subject would be subjected to torture or inhuman treatment. This has been the main provision for balancing the interference with data protection and privacy and ensuring that law enforcement access clauses will not put third-country nationals in a more dangerous situation than they already are.

Also, as another safeguard, all requests by law enforcement authorities and the processing operations regarding those requests will be documented to monitor the lawfulness of the requests.

It can be said that there is most probably no discrimination of asylum seekers, as there is no beneficial treatment of certain groups of people. Nevertheless, there are significant concerns of misuse of the EURODAC by the relevant authorities. It is not clear also how the law enforcement bodies really do benefit from the usage of the database. Asylum seekers are stigmatized because of the fact that their fingerprints are in the database.

In order to avoid these problems, the usage and access to the database has to be well motivated, it can be done only in rare cases and should not be a normal procedure in criminal investigations. Using EURODAC should be rather an exception than a rule for the law enforcement authorities.

Associate Professor Dr. **Lehte Roots** is head of the Chair of Public Law in Tallinn Law School of Tallinn University of Technology. She received her PhD from European University Institute in Florence, Italy. She has a master's degree in Public Management from Potsdam University and a Master in Research degree from European University Institute. During her career she has been a project leader of several research and practical projects, has held management positions in the private sector, NGOs, research institutions, also at the international level. She has been Estonian expert in several research projects funded by the European Commission, the European Parliament and conducted by network of experts. She has published articles and book chapters, presented at conferences about migration, asylum, citizenship, good governance, enlargement, and public sector reforms.

References

Aas, K. F. (2006), "'The body does not lie': Identity, risk and trust in technoculture," *Crime Media Culture*, vol. 2, pp. 143–158. http://dx.doi.org/10.1177/1741659006065401

Boehm, F. (2012a), 'Data processing and law enforcement access to information systems at EU level,' *Datenschutz und Datensicherheit*, vol. 36, no. 5, pp. 339–343. http://dx.doi.org/10.1007/s11623-012-0131-5

—— (2012b), *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-level*, Berlin & Heidelberg: Springer. http://dx.doi.org/10.1007/978-3-642-22392-1

Boehm, F. & Cole, M. D. (2014), *Data Retention after the Judgement of the Court of Justice of the European Union.* Retrieved from http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf [accessed 15 Mar 2015]

Council of the European Union (2000), Council Regulation (EC) No. 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, *Official Journal of the European Union*, L 316, 15.12.2000.

—— (2008a), Policy Plan on Asylum—An Integrated Approach to Protection Across the EU, COM(2008) final 360, 17.6.2008.

—— (2008b), Commission proposal for a Regulation of the European Parliament and of the Council concerning the establishment of EURODAC for the comparison of fingerprints for the effective application of Regulation (EC) No. […/…], COM(2008) 825, 3.12.2008.

—— (2009), Note of the Meijers Committee, on the amended proposal for the Eurodac Regulation (COM(2009) 342) and the Decision on requesting comparisons with Eurodac Data for law enforcement purposes, 30.12.2009.

—— (2012), Note by the Meijers Committee on the amended proposal for a Regulation on the establishment of EURODAC, COM(2012) 254, 10.10.2012.

—— (2013), Council Regulation No. 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 Council Regulation No. 604/2013, *Official Journal of the European Union*, L 180, 29.6.2013.

EDPS (2010), Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints, *Official Journal of the European Union*, C 92, 10.4.2010.

—— (2011), Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on migration, 7.7.2011.

—— (2012), Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No [603/2013] (Recast version), 5.9.2012.

EURODAC (2013), EU 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 (EU) No. 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on

requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No. 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast), *Official Journal of the European Union*, L 180, 29.6.2013, pp. 1–30.

Impact Asssessment (2009), Commission Staff Working Document Accompanying the amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of EURODAC and to the proposal for a Council decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes, SEC(2009) 936, 10.9.2009.

Farraj, A. (2010–2011), 'Refugees and the biometric future: the impact of biometrics on refugees and asylum seekers,' *Columbia Human Rights Law Review*, vol. 42, no. 3, pp. 891–941.

Kindt, E. J. (2013), *Privacy and Data Protection Issues of Biometric Application: A Comparative Legal Analysis*, Dordrecht, etc.: Springer.

Liu, Y. (2008), 'Identifying legal concerns in the biometric context,' *Journal of International Commercial Law and Technology*, vol. 3, no. 1, pp. 45–54.

van der Ploeg, I. (1999), "The Illegal Body: 'Eurodac' and the Politics of Biometric Identification," *Ethics and Information Technology*, vol. 1, no. 4, pp. 295–302. http://dx.doi.org/10.1023/A:1010064613240

Pugliese, J. (2013), 'Technologies of Extraterritorialisation, Statist Visuality and Irregular Migrants and Refugees,' *Griffith Law Review*, vol. 22, no. 3, pp. 571–597. http://dx.doi.org/10.1080/10383441.2013.10877013

Stefanou, C. & Xanthaki, H. (2008), *Towards a European Criminal Record*, Cambridge: Cambridge University Press. http://dx.doi.org/10.1017/CBO9780511495069

Thomas, R. (2005), 'Biometrics, International Migrants and Human Rights,' *European Journal of Migration and Law*, vol. 7, no. 4, pp. 377–411. http://dx.doi.org/10.1163/157181605776293255

UNHCR (2012), An efficient and protective Eurodac: UNHCR comments on the Commission's amended proposal for a Regulation of the European Parliament and of the Council on the establishment of Eurodac for the comparison of fingerprints for the effective application of the Dublin regulation [...], (2012 November). Retrieved from http://www.refworld.org/docid/50ad01b72.html [accessed 13 Mar 2015]

—— (2013), Moving forward on asylum in the EU: UNHCR's Recommendations to Ireland for its EU Presidency January–June 2013. Retrieved from http://www.unhcr.org/50e40d9f6.html [accessed 13 Mar 2015]