The impact of the new Proposal of Eurodac on asylum seekers: threats and tendencies in the right to privacy and data protection

Jorge Agustin Viguri Cordero
PhD Candidate (Scholarship granted by Generalitat Valenciana)
Constitutional Law, Department of Public Law
Universitat Jaume I (UJI)

Summary

The "European Dactyloscopy" Information System (Eurodac), reformed by the current Eurodac Regulation (EU) No. 603/2013, is the main and indispensable element to increase significantly the efficiency of the procedure within the Common European Asylum System (CEAS).

On April 6, 2016, the European Commission (EC) proposed to reform the CEAS and one month later, adopted the first package of proposals for CEAS reform including, among others, a Proposal for a regulation to reform the Dublin system and a Proposal for a regulation to amend Eurodac.

The aforementioned reform seeks to address the current challenges, in particular, the prevention of the massive flow of illegal immigrants. For this purpose, it pursues greater efficiency and an improved control of applicants for international protection. However, this reform also impacts on the rights and guarantees in the field of privacy and protection of personal data of this vulnerable group. Firstly, the scope of application is extended to identify and have access to irregular migrants' personal data. Secondly, the Proposal also extends the categories of personal data including not only the collection of fingerprints but also facial recognition systems with the digital photograph. Thirdly, the Proposal maintains the strict conditions of law enforcement access to personal data. It, indeed, reinforces the guarantees to the information rights of the data subject.
These reforms intend to considerably improve the effectiveness of the international protection procedure in the fight against international criminality, terrorism and other

security threats, but have a strong impact on the fundamental rights of applicants for international protection, and in particular their right to privacy and data protection.

1. Introduction

The implementation of information systems in border management is not new. Member states have been adopting technological measures for the collection, management and processing of personal data in a massive way since the 1990s, in order to facilitate mobility on an unprecedented scale and early detect any factor that prevents the entry of unauthorised or unwanted immigrants.

The *fortress model*[1] has been complemented by an overlay of information systems that have been identifying unwanted immigration. This new tendency towards more complex and intelligent border mechanisms has been accompanied by a further set of provisions that aim at maintaining the integrity and security of Member States, which is gradually breaching fundamental rights of asylum seekers.

The *European Dactyloscopy System* (*Eurodac*) was created through Regulation (EC) 2725/2000 to identify asylum seekers and prevent irregular immigration, which is currently reformed by the Eurodac regulation (EU) No. 603/2013[2]. This can be considered as the main technical instrument that complements the Dublin III regulation No 604/2013[3]. This Regulation pursues the objective to determine the Member State

[1] Chad C. Caddal, *People Crossing Borders: An Analysis of U.S. Border Protection Policies Congressional Research Service*, May, 2010, p. 8. Available at: https://fas.org/sgp/crs/homesec/R41237.pdf. Accessed on February 2, 2018.

[2] Regulation (EU) 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 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. *OJ L 180, 29.6.2013, p. 1–30*

[3] Regulation (EU) No 604/2013 Regulation 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. *OJ L 180, 29.6.2013, p. 31–59*

responsible for examining the asylum application and, for that purpose, uses the data entered previously in Eurodac.

Consequently, Eurodac might be defined as the key and indispensable database to increase the efficiency of the procedure within the Common European Asylum System (CEAS), especially in the face of the need to tackle the massive influx of migrants and refugees.

At the height of the refugee crisis in 2015, the operability of this information system marked a turning point. According to the risk analysis carried out by Frontex in 2016, around 1 million people travelled in the EU in 2015 without the proper travel documents[4]. The Greek authorities estimated that no more than a third of the people arriving on the Greek islands were fingerprinted. Similarly, the German authorities in the Bavarian region admitted publicly in 2015 that they could not take fingerprints to every asylum applicant.

This situation could have originated as a result of the implementation of the Dublin III System, which excluded *de facto* the interests and personal needs of the applicants for international protection[5].

This rigidity of the system did not encourage applicants to voluntarily submit their fingerprints. In fact, if they applied for asylum in the first country of entry into the EU, they would be subjected to decisions issued by the border authorities of the Member States (which frequently supported disproportionate asylum applications). In fact, certain Member States such as Greece and Italy tended to avoid the registration of applicants in

---

[4] Frontex, *Risk analysis for 2016*, p. 17. Available at: http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annula_Risk_Analysis_2016.pdf. Accessed on February 18, 2018.

[5] This situation of pressure faced by applicants for international protection delayed in accessing the asylum procedure and the lack of integration prospects in Italy. For further information, see: UNHCR *Recommendations on Important Aspects of Refugee Protection in Italy*, July 2013. Available at: http://www.unhcr.org/protection/operations/500950b29/unhcr-recommendations-important-aspects-refugee-protection-italy.html Accessed on March 15, 2018.

order to minimize the likelihood of being responsible in accordance with the Dublin system[6].

As a consequence, a particularly serious scenario for the security of the Member States originated due to a wide range of causes: general lack of identification, the high risk of unauthorized secondary movements and generalised irregular stays within the EU[7].

All of these circumstances led the European Commission (EC) to highlight the chaotic situation that member states suffered since the widespread "invisibility" of a large number of unidentified migrants in some member states. On April 6, 2016, the EC proposed a reform of the CEAS as a whole[8]. Furthermore, the European Parliament also highlighted the problems arising from its application in a briefing on Eurodac's legislative reforms[9].

As a result, the new proposal for an Eurodac Regulation[10] aims to strengthen the protection of fundamental rights (in particular, respect for private life, privacy and protection of personal data that is regulated in articles 8 and 52.3 CFREU and article 8 ECHR) solving a fragmented EU system which is associated to national security issues

---

[6] European Council on Refugees and Exiles (ECRE), "Hotspots": the Italian example – conversation with Christopher Hein from CIR" 2nd October 2015. Available at: https://www.ecre.org/hotspots-the-italian-example-conversation-with-christopher-hein-from-cir/ Accessed on 5 February, 2018.

[7] European Commission, Migration and Home Affairs, *Identification of applicants* (EURODAC). Available at: https://ec.europa.eu/home-affairs/what-we-do/policies/asylum/identification-of-applicants_en Accessed on 5 February, 2018.

[8] European Commission, «Communication from the Commission to the European Parliament and the Council towards a Reform of the Common European Asylum System and Enhancing Legal Avenues to Europe», COM (2016) 197 final. Information available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-migration/proposal-implementation-package/docs/20160406/towards_a_reform_of_the_common_european_asylum_system_and_enhancing_legal_avenues_to_europe_-_20160406_eh Accessed on 12 February 2018.

[9] European Parliamentary Research Service (EPRD), Recast Eurodac Regulation, March 10, 2017. Information available at: http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589808/EPRS_BRI%282016%29589808_EN.pdf Accessed on 14 February 2018.

[10] European Commission, Proposal for a on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast) 4.5.2016 COM, 2016, 272 final.

and that, in the light of experience, can be classified as inefficient and limited in the protection of rights[11]. This evidences the need to address a study about the expected amendments to the current legal framework in order to highlight the effective degree of protection, its deficiencies as well as improvements that guarantee the protection of the personal data of applicants for international protection.

2. Data protection issues in the new proposal for a Eurodac Regulation

2.1. The collection and processing of personal data in Eurodac

One of the main novelties of the Eurodac Proposal with respect to the current Eurodac Regulation (EU) No. 603/2013 is the greater efficiency and control of the applicants for international protection. This is a prevailing need in the Member States that lowers guarantees in the privacy and protection of personal data of asylum seekers for reasons of prevention, detection and investigation of serious crimes and terrorism.

The scope of searches is extended in the new Proposal. According to articles 15 and 16, immigration authorities will be able to compare and transmit all categories of personal data about applicants for international protection, third-country nationals who are in an illegal situation and also immigrants who have entered irregularly into the EU territory.

This is particularly relevant since immigration authorities from different Member States also collect personal data, exceeding the Eurodac main objective of providing and increasing effective identification. It can constitute a potential risk to function creep[12], which interferes with the right to data protection provided in article 8 ECHR.

The procedure tends to gather all information and personal data available to examine the application for international protection. In this regard, authorities may verify whether there may be any reason that may collide with the national interest to ensure security and public order within the EU borders.

---

[11] F. 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*. Berlin: Springer, 2011, p. 28.

[12] The principle of function creep has been studied by E. Brouwer, "Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation" in L. Besselink, F. Pennings y S. Prechal (eds.), *The Eclipse of the Legality Principle in the European Union, Kluwer Law Internacional*, 2011, pp. 273-294.

In my view, a conflict of interest arises from a double dimension. The practices of mass storage of personal data might be necessary to ensure national security but may also imply an intrusive practice in the privacy of the applicants, which runs counter to the principle of proportionality and purpose limitation[13]. As a consequence of this potential breach, the Proposal for a Eurodac Regulation aims to extend its purpose, making its main objective more flexible. According to Recital 20 Proposal of Eurodac Regulation[14], Member States will have greater flexibility in the weighting of the necessity, proportionality and purpose limitation principles to achieve the objectives of general interest concerned.

In order to counteract this greater scope of the Proposal in the collection of personal data, the rights of information of the data subject are reinforced (Article 30 of the Proposal). The authorities of the Member States must exhaustively comply with a series of new or partially planned obligations in article 29 Eurodac Regulation. For example, authorities need to ensure that applicants understand (or are reasonably supposed to understand) a series of rights in the field of data protection[15]. For this reason, a high level of formality is required including concise, transparent, intelligible and easily accessible information, even using clear and plain language to guarantee the highest standards of understanding.

---

[13] Article 5.1 b) General Data Protection Regulation (GDPR) states that *personal data collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*. According to the above-mentioned Proposal, *privacy by design* principles shall be implemented as they are proportionate in terms of the right to protection of personal data. This principle does not require the collection and storage of more data than is absolutely necessary to allow Eurodac to function and meet its aim. Further information can be found at: Proposal for a Regulation on the establishment of 'Eurodac'... *op. cit.*, p. 8.

[14] Recital 20 Proposal of Eurodac Regulation states the following: (...) *In line with the requirements of Article 52(1) of the CFRUE any such interference must be in accordance with the law, which must be formulated with sufficient precision to allow individuals to adjust their conduct and it must protect individuals against arbitrariness and indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise. Any interference must be necessary to genuinely meet an objective of general interest and proportionate to the legitimate objective it aims to achieve.*

[15] According to article 30 Proposal of Eurodac Regulation, authorities in Member states shall provide the following information: the identity of the controller and contact details of the data protection officer, the purpose for which his or her data will be processed in Eurodac, the recipients or categories of recipients, the obligation to have his or her fingerprints taken, the period for which the data will be stored, the existence of the right to request from the controller access to data relating to him or her, and the right to request that inaccurate data relating to him or her be rectified and the completion of incomplete personal data or that unlawfully processed personal data concerning him or her be erased or restricted, 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

Nevertheless, despite an increased protection in the collection of information, the techniques employed for processing personal data still remains lower than expected. Member States tend to prioritise their national security undermining the guarantees of asylum seekers. Consequently, it is important to strike a balance between effective management of asylum applications and the improvement in the legitimate rights and interests of this vulnerable group[16].

National security has become an argument for adopting measures that limit fundamental rights instead of ensuring enforcement of the law[17]. This is a complex weighing which seem to be opposed to one another, but in fact they complement each other to achieve both objectives: safeguarding the interests of national security, and the profound respect for the CEAS, including the right to privacy and the protection of the personal data of the applicants for international protection.

2.2. The processing of the biometric data

The protection of data on biometric data is, in my opinion, one of the basic aspects in the Eurodac database. The new General Data Protection Regulation (RGPD) defines biometric data in article 4 (14) as *personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.*

Therefore, the nature of personal data according to article 9 GDPR requires the highest level of protection. Thus, the treatment of the typology of sensitive personal data shall be, as a general rule, prohibited. These identification data are on an equal footing with the personal data that reveals racial or ethnic origin, political opinions, religious or

[16] García Mahamut, R.. «La ductilidad del derecho a la protección internacional (refugio y protección subsidiaria) ante las crisis humanitarias: un desafío para Europa y para el Sistema Europeo Común de Asilo». *Teoría y Realidad Constitucional*, núm. 38, 2016, p. 237.

[17] Serra Cristóbal, R, «Los derechos fundamentales en la encrucijada de la lucha contra el terrorismo yihadista: Lo que el constitucionalismo y el derecho de la Unión Europea pueden ofrecer en común». En *Teoría y realidad constitucional*. núm. 38, 2016, p. 488.

philosophical beliefs, among others, that not only proves the reasons of persecution but also justify the application of international protection.

However, paragraph 2 g) directly excludes from the prohibition in the processing of sensitive data a compelling public interest reason. This is the case in the management of applications for international protection as the same section imposes a limit that is determined through proportionality to the aim pursued, respects the essence of the right to data protection and provides suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Nowadays, Eurodac Regulation only enables comparison of the fingerprints of asylum seekers and illegal immigrants. The collection of such dactyloscopic and sensitive data aims to ensure the initial objetive to operate exclusively with fingerprints, without keeping other personal data apart from the sex of the person (articles 2, 15 and 16 Eurodac Regulation).

In October 2013, the United Nations High Commissioner for Refugees (UNHCR), implemented a Biometric Identity Management System (BIMS). It underlined for the first time the importance of collecting new biometric data as an accurate way to verify identities using unique physiological characteristics. To that purpose, UNHCR aimed to include not only fingerprints but also new data such as the iris and facial features[18]. The insertion of new biometric data led the European Agenda Migration in 2015 to propose at this stage amendments to the operation of Eurodac database in order to face new challenges faced by Member States in the frontline of migrant arrivals[19].

Fingertips damages motivated the extension of biometric data, because they usually caused non-compliance in the process of identification. However, the frequent margins

[18] United Nations High Commissioner for Refugees (UNHCR), «*Biometric Identity Management System. Enhancing Registration and Data Management*». More information can be found at: http://www.unhcr.org/550c304c9.pdfAccessed on 15 February 2018.

[19] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions «*A European Agenda on Migration*», COM, 2015) 240 final, May 2015, pp. 13 y 14.

of errors[20] in the fingerprinting process were not specified, which also constitutes, in my view, one of the causes to extend the collection of other biometric data.

As a result, the Eurodac Proposal formally expands in article 2 the typology of personal data to facial images, which underlines serious concerns in the field of data protection and privacy for persons seeking international protection in Member States[21]. Specifically, the Proposal would oblige national authorities to take the fingerprints and facial images of persons seeking for international protection, third-country national or stateless persons that not only are apprehended by the competent control authorities in connection with the irregular crossing by land, sea or air, but also those found illegally staying within its territory. Besides, Member States shall transmit all of these data electronically (article 25 Proposal Eurodac Regulation).

The collection of facial images will be the pre-cursor to introducing facial recognition software in the future. The legal nature of this information system will undergo a substantial transformation. However, we cannot fail to be struck by the fact that the main purpose is not to increase the efficiency of the system or to reduce the margin of errors, but *to reduce the need for additional communication infrastructure between Member States to share information on irregular migrants that have not claimed asylum*[22]. This can be catalogued as a *technological paranoia*[23] that follows the implementation of more accurate identification techniques. However, they may be excessive to simply determine the Member State responsible for examining an application for international protection.

---

[20] An study about the error rate in Eurodac database can be found in: Kenk, V.S., Križaj,, J., Štruc, J. & Dobrišek S., Smart Surveillance Technologies in Border Control, in European Journal of Law and Technology, Vol 4., No. 2., 2013. http://ejlt.org/article/view/230/378. Maghiros, I. e.a. Biometrics at the Frontiers: Assessing the Impact on Society, in European Commission, Joint Re-Search Centre and Institute for Prospective Technological Studies (eds.), Technical Report Series, 1 June 2005, p. 166.

[21] The Proposal would oblige to national authorities to take the fingerprints and facial images of persons seeking for international protection, third-country national or stateless persons that not only are apprehended by the competent control authorities in connection with the irregular crossing by land, sea or air but also those found illegally staying within its territory. Member States shall transmit all of these data electronically (article 25 Proposal Eurodac Regulation).

[22] European Commission, Proposal for a on the establishment of 'Eurodac', *op. cit.*, p.5

[23] Alterman, A., 'A piece of yourself: Ethical issues in biometric identification', Ethics and Information Technology, Vol. 5, 2003, (139-150), p. 146.

Up until now, the collection of facial images will be a *pilot test* to introducing facial recognition software in the future. The European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Eu- Lisa) will have a very important role in its implementation. By 2020, this Agency should conduct a report on the technical feasibility of adding facial recognition software to the Central System. However, once the new Central System is operational, Eu-LISA should submit to the European Parliament, the Council and the Commission a report on the activities of the Central System.

The extension of biometric data may ensure reliable and accurate results following a comparison of facial image data, which, compared to other personal data, have a very little margin of error. Therefore, they are accurate to determine the exact identity of the applicants, especially if several biometric data are cross-matched to verify their identities.

As a result, the collection of these sensitive data suffers from important amendments in the new Proposal Eurodac Regulation. It lowers the age of taking fingerprints from 14 to 6 years old (articles 10, 13 and 14 of the Proposal Regulation Eurodac) and introduces the obligation to store the names; date of birth, nationality, the Member State of origin or allocation, the details of the identity or travel document and the biometric data (Recitals 31, 35 and Article 2 Proposed Regulation).

In this sense, the risks or benefits of this extensive use of biometric identifiers and their impact on the fundamental rights of applicants for international protection are still unknown. However, two major challenges should be highlighted. On the one hand, the inclusion of biometric data in the Eurodac database with additional sensitive information (for example, information relating to human health) requires the highest level of security and protection in the light of the new General Data Protection Legislation (GDPR)[24]. On the other hand, the exchange of this sensitive data will not always respect the high guarantees set forth in the GDPR because of its close connection with national security.

[24] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *OJ L 119, 4.5.2016, p. 1–88.*

The Directive on data protection in the area of police and justice[25] may also be applicable to applicants for asylum whose safeguards are considerably weakened[26].

Fortunately, the new Dublin IV Proposal establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection[27] expressly states in Recital 38 that the new GDPR applies to the processing of personal data by the Member States. This evidences that national authorities shall comply with the high conditions laid down in the GDPR. Member States may stipulate that data subjects' rights may be exercised only in accordance with the Directive on data protection in the area of police and justice.

2.3. *Law Enforcement Access to Eurodac*

The current Eurodac Regulation[28] already provides for the access Eurodac to the law enforcement authorities (national enforcement bodies and Europol) for the purpose of prevention, detection and investigation of terrorist offences and other serious criminal offences which is also adopted in the Proposal (articles 21, 22 Eurodac Regulation and 22, 23 Proposal).

---

25 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. *OJ L 119, 4.5.2016, p. 89–131*.

[26] Article 10 (a) of the Directive (EU) 2016/680 allow the processing of biometric data only if they are strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only where authorised by Union or Member State law.

[27] 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 (recast), COM(2016) 270 final. 2016/0133 (COD).

28 Regulation (EU) 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 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. *OJ L 180, 29.6.2013, p. 1–30*

In addition, the new Proposal aims to control illegal immigration to and secondary movements within the EU, and to contribute to improve the effectiveness of the EU return policy.

In fact, the access to personal data for applicants for international protection was analysed by the UNHCR [29] and the European Data Protection Supervisor (EDPS) [30], which highlighted the potential adverse effects it may have on innocent persons. Thus, this access fell outside the intended scope of the Regulation (providing an effective way to apply for asylum in the EU). Concerning the right of access to the Eurodac database, the new Proposal maintains the strict conditions of access as designated law enforcement authorities may only request access to the system data if there are reasonable grounds to consider that will substantially contribute to the prevention, detection or investigation of the criminal offence in question.

The Proposal also sets out a series of improvements with respect to the law enforcement access. On the one hand, greater guarantees are granted to the rights of information of the data subject, and expressly provides for the completion of personal data (article 30.1 (f) Proposal). On the other hand, it foresees one of the major limitations in terms of access: the principle of subsidiarity. This principle establishes that access should be allowed only on condition that comparisons with the national fingerprint databases of the Member State and with the automated fingerprinting identification systems of all other Member States (Recital 42) and prohibits systematic comparisons of personal data contained in Eurodac (Recital 41).

All in all, law enforcement access to Europol database may interfere with the fundamental right to private life, since it exceeds the limits set by the principle of proportionality and

---

[29] United Nations High Commissioner for Refugees (UNHCR), *An efficient and Protective Eurodac*, November 2012. The information is available at: http://www.unhcr.org/50adf9749.pdf Accessed on 20 March, 2018

[30] European Data Protection Supervisor, 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), September 2012. Available at: https://edps.europa.eu/sites/edp/files/publication/12-09-05_eurodac_en.pdf Accessed on 20 March, 2018.

purpose limitation. This access, indeed, can be classified as a potentially discriminatory tool because it allows access to data to prevent or investigate the commission of a serious crime or terrorist attack. Besides, the mere possibility that law enforcement access to Eurodac implies that the applicants can be identified from a crime scene if their biometric data is found (this possibility does not exist for other categories of persons). This may result in an increased stigmatisation of applicants for international protection, a group of vulnerable persons who are suspected of criminality[31], which is manifestly contrary to the values in the CEAS, CFREU and international standards, including the 1951 Geneva Convention and 1967 Protocol.

It cannot be concluded that law enforcement access presumes *per se* the commission of an offence. Nevertheless, the provision articulates the mere possibility that law enforcement authorities can access to different categories of personal data justifying national security reasons in a vague and abstract manner. This can be considered an excessive intrusion on the privacy of applicants for international protection protected by virtue of the principle of necessity, which requires an exhaustive identification in order to confront the terrorist threat or to prevent an offence from being committed or going unpunished.

Finally, although the new Eurodac Proposal for a Regulation increases the guarantees on access to the data contained in Eurodac, they are closely bound by the maintenance of the generalised objective of detecting illegal immigration to the EU, secondary movements and the prevention, investigation, detection or prosecution of criminal offences or other serious crimes (Recital 13 of the Proposal). In this context, the EC will examine the legal framework for access to Eurodac in order to revise the legal framework for law enforcement access to Eurodac.

3. Conclusions

[31] Vavoula, N,. The recast Eurodac Regulation: Are Asylum Seekers Treated as Suspected Criminals, in: Céline Bauloz, Meltem Ineli-Ciger, Sarah Singer and Vladislava Stoyanova (eds.): S*eeking Asylum in the European Union*, 2015, p. 261.

The Eurodac Information System has undergone a substantial transformation in recent years. Originally, it only collected asylum seekers' fingerprints, but the current Eurodac Regulation (EU) No. 603/2013 foresees access to national authorities and personal Europol, evidencing a greater scope in the field of privacy and data protection of this group.

Overall, the impact of the new proposal for Eurodac regulation is expected to be wider. This information system will no longer be anonymous and with little relevance in terms of data protection, but will become a real database of asylum and irregular immigration. The scope of application of Eurodac will be extended in order to identify not only third-country nationals in an irregular situation in the EU, but also immigrants who have entered irregularly into the EU territory. In addition, it considerably lowers the age of taking fingerprints from 14 to 6 years old. Likewise, Eurodac formally expands the typology of personal data as it aims at storing names, date of birth, nationality, the Member State of origin or allocation, the details of the identity or travel document and the biometric data (including not only fingerprints but also digital photographs).

This trend towards an increased collection of personal data reinforces the management of the Union's external borders to better contain the growing flows of illegal migration and provide an effective CEAS procedure. National authorities may place greater emphasis on research, data collection and analysis to determine the personal identity of different groups of persons including applicants for international protection. However, this tendency to gather more personal data may cause an intolerable practice in the system nowadays. The authorities tend to collect all the personal data available within the international protection procedure. On the other hand, the refusal of the subjects to provide all their personal data is considered a presumption of irregularity for national authorities, which may provoke a crisis of confidence in our democratic system.

It is also important to highlight that the lack of clarity and the shortcomings in the current data protection legislation in the field of international protection create a situation of legal uncertainty that could cause damages for breaches of privacy. As previously stated, Dublin IV Proposal only states in Recital 38 that the new GDPR applies to the processing

of personal data by the Member States, which evidences that national authorities shall comply with the high conditions laid down in the GDPR but they have great flexibility in decreasing legal guarantees. Consequently, they may stipulate in their national legislation that data subjects' rights may be exercised only in accordance with the Directive on data protection in the area of police and justice due to its links to national security and public order.

Additionally, concerning to Law Enforcement Access to Eurodac, the Proposal maintains the strict conditions of access by law enforcement authorities to personal data. However, the Proposal fortunately introduces the principle of subsidiarity, which implies that these bodies must access the database as a last resort in order to reduce the potential discrimination of this group with respect to other categories of persons, especially in the context of a criminal investigation.

Finally, Eurodac will become a key information system in the processing of personal data in the near future. Its extension responds to the purpose of preventing, detecting and investigating serious crimes and terrorism. This proposal becomes much more «intrusive» in the sense that it seeks to protect and guarantee national security and public order, which gives the Member States greater flexibility as far as their compliance with current provisions in the field of data protection is concerned.