



ΕΥΡΩΠΑΪΚΟ ΚΕΝΤΡΟ ΑΡΙΣΤΕΙΑΣ JEAN MONNET
ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

JEAN MONNET EUROPEAN CENTRE OF EXCELLENCE
NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS

Co-funded by the
Erasmus+ Programme
of the European Union



Migrants' human rights facing surveillance technologies in immigration enforcement

ELENI GIANNAKOU

SEPTEMBER 2021



Copyright 2021

JEAN MONNET EUROPEAN CENTRE OF EXCELLENCE
NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS
21-23 Marasli str. , 106 76 Athens
Tel: +30 210 72 20 508
Email: jmcenter-athens@pspa.uoa.gr, www.jmce.gr

All rights reserved

The Jean Monnet European Center of Excellence does not adopt policies or other positions. In fact, it makes an effort to present in the context of its activities and as far as possible all the existing views. The analysis and thesis published in all editions of the European Center for Excellence Jean Monnet should be attributed solely to the authors themselves and should not necessarily reflect the views of the Center, its Board of Directors, management or, as the case may be, in any way cooperating bodies.

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Eleni Giannakou¹

Summary

Artificial Intelligence (AI) and surveillance technologies are developing fast and becoming part of the migration policies. AI is a strategic technology that offers benefits, but also poses threats to fundamental rights and values. This study questions the compatibility of surveillance and biometrics' technologies with the rights of privacy, presumption of innocence, liberty, non-discrimination and with the principal of good administration.

Computers' outputs are regarded as rational and infallible, so people tend to use them as decision tools. If this occurs in migration-related decisions, the results in human rights protection will be grave. Besides the detrimental effects on individuals, who could be given an unjust reply to their asylum application, the consequences of flawed decision-making will influence the effectiveness of border systems per-se and jeopardise the protection of fundamental rights. Additionally, the impact of new surveillance and identification technologies affects disproportionately the minority ethnic communities, causing or strengthening structural inequality.

While acknowledging the importance of existing legal tools to mitigate the risks of AI and surveillance technologies, it is vital to underline that the non-discrimination and data protection laws need to be supported by regulatory safeguards and redress mechanisms. This study reviews EU Directives and Regulations, reports from NGO's and via a critical eye on present bibliography, draws conclusions on the robustness, pitfalls and possible ameliorations of the migration policies.

¹ Eleni Giannakou is a last year undergraduate law student at National and Kapodistrian University of Athens, Greece. She is interested in environmental law, migration law and human rights, subjects that she studies in the light of sociolegal studies and feminist analysis. She has taken online courses on International Immigration from the University of Oxford and continues to broaden her knowledge by attending seminars and lectures. She has been a Researcher in International Law at SAFIA and member of the Advocacy Team of ELSA Greece to promote human rights and the rule of law.



Table of Contents

- Summary 1
- 1.Introduction 5
- 2. **Errors and abuses in surveillance and biometrics technologies**..... 6
 - 2.1. **Interoperability: inaccurate data and the right to effective remedy.** 7
 - 2.2. **Collecting data from minors in registration procedures** 9
 - 2.3. **The problem of compromised informed consent.**..... 12
- 3. **Protection of personal data and the discriminatory aspects of interoperability framework** 13
 - 3.1 **Impact on migrant communities.**..... 16
 - 3.2. **Non-discrimination principle and AI: the facial recognition example and biased sample** 18
 - 3.3 **AI’s possible repercussions in collective and individual enjoyment of migrants’ human rights.**..... 19
- 4 **‘Firewalls’ between public services and immigration enforcement and the issue of accountability**..... 22
- 5 **Legal framework and recommendations**..... 25
- 6 **Conclusion**..... 30
- Bibliography** 32

1.Introduction

Human rights safeguards prove their importance when they are challenged by adverse conditions. Likewise, the development of technology shows its full spectrum of possibilities when questions of ethics and lawfulness arise. Given that technology is a tool that can be used differently depending the legal environment that regulates its application, it is important to examine technology's application in humanitarian and forced migration circumstances.

In 23rd September 2020 the new [European Pact on Migration and Asylum](#)² was published, aiming to ameliorate the EU's control over migration and deal with past fallacies. Among others, the Pact proposes creating and expanding biometric databases and access to data of third country nationals³. In the same year, 2020, EU's border agency FRONTEX⁴ was [granted](#) a €5.6 billion budget (M. Douo, L. Izuzquiza, M. Silva, 2021), the largest among any EU agency. This growth in funds leads to increased powers and comes along with the European Pact's objective for greater border control based on more firearms and biometric surveillance. The major human rights implications derived from both from the Pact's proposals and the Frontex's expansion are shaping EU's border control regime. Existing and proposed regulations seem to fail to protect fairness and human rights form AI's misuse in migration processes.

There is need to work towards ameliorating asylum and migration procedures, with the intention of constructing fair, efficient, compliant with rights, and adequately resourced instruments. This study questions the compatibility of surveillance and biometrics' technologies with the rights of privacy⁵, presumption of innocence⁶, liberty⁷, non-discrimination⁸ and with the principal of good administration⁹. While acknowledging the importance of existing legal tools to mitigate the risks of Artificial intelligence (AI) and

² European Commission New Pact on Migration and Asylum COM(2020) 609 final, 23 September 2020, 21–22.

³ Articles 4(2), 9, 10 12, 13 14 and 14a of the amended Proposal for a Eurodac Regulation, and Article 10, 11 13, 14 and 14a of the Proposal for a Regulation introducing a screening of third country nationals at the external borders.

⁴ Budget 2020/ VOBU Frontex - European Border and Coast Guard Agency Warsaw, 01/01/2020 www.frontex.europa.eu

⁵ Article 8 of the EU Charter of Fundamental Rights (Respect of privacy and family life) OJ C 202, 7.6.2016, p. 395–395, Article 8 of the European Convention on Human Rights [ECHR], Article 12 of the Universal Declaration of Human Rights

⁶ Article 48 of the EU Charter of Fundamental Rights Official Journal of the European Union C 303/17 - 14.12.2007, Article 6(2) and (3) of the ECHR, Article 11 of UN's Universal Declaration of Human Rights.

⁷ Article 6 of EU Charter, Article 5 ECHR, (Right to liberty and security)

⁸ Article 21 of the EU Charter of Fundamental Rights, Article 14 of the ECHR and on Article 1 of Protocol No. 12 to the Convention, Article 7 Universal Declaration of Human Rights

⁹ Article 41 EU Charter of Fundamental Rights Official Journal of the European Union C 303/17 - 14.12.2007.

surveillance technologies, it is vital to underline that non-discrimination law and data protection law need to be supported by regulatory safeguards and redress mechanisms.

A transparent legal framework is necessary in order to (1) put down clear guidelines about policing and the use of personal data, (2) precisely define the specific legal thresholds that could justify access to the people's data, (3) ensure accountability for the implications of digital technology and data processing for human rights and discrimination, (4) provide access to effective legal remedies, (5) establish “firewalls” to ensure that personal data obtained when undocumented people access health care or social services is not used in their expense (Ch. Jones, 2020). If there is a lack of such a legal foundation, the deployment of cutting-edge technology and equipment is undermining the fundamental rights of travelers, migrants, and refugees.

This study discusses the problematic aspects in interoperability of EU large-scale databases, as well as AI limitations under the scope of migration policies. It does so via presenting reports and articles from up-to-date official sources and analyzing present legal framework, as well as its potential ameliorations. The current legal approach to regular and irregular migration is based on a criminal justice model and perpetuates discrimination and inequalities. This regulatory vision and its methods determine the use of technology and technology's impact on rights of people in movement. Without questioning the foundations of migration policies, we examine them with a critical eye, in order to propose a sharper oversight on national and international migration mechanisms, an oversight grounded on fundamental human rights.

2. Errors and abuses in surveillance and biometrics technologies

Algorithms are not perfect, neither per se democratic nor neutral. It is essential to guard their transparency, to ensure accountability from discrimination, bias, and error. On this chapter it will be analysed that, on the one hand, data can be incorrect, on the other, the decisions based on them can be even unlawful. Decisions regarding immigration are complex and the migration stories opaque (Molnar, 2019). AI systems are not capable to provide as nuanced and just outcomes as required. Besides the detrimental effects on individuals, who could be given an unjust reply to their asylum application, the consequences of flawed decision-making influence the effectiveness of border systems per-se and jeopardies the protection of fundamental rights. Additionally, the impact of new surveillance and

identification technologies affects disproportionately the minority ethnic communities, causing or strengthening structural inequality.

2.1. Interoperability: inaccurate data and the right to effective remedy.

Interoperability between EU information systems is an initiative introduced with the aim of facilitating identity checks of non-EU nationals, documented or undocumented. Different authorities are given access to a network that links both current and future EU databases. Authorities verify the identity of a particular individual and examine all the available information for this person by searching multiple systems at the same time. The Common Identity Repository¹⁰ (CIR) would be that new database containing biographic and biometric data (Jones, 2019), with a capacity to store up to 300 million records collected from existing and forthcoming EU databases (E.Brouwer, 2019).

Interoperability causes concerns regarding (a) automated decisions based on the databases' information and the right to an effective remedy, (b) discriminatory processes and (c) incompatibility with the EU's approach to the protection of personal data.

The framework for interoperability is establishing with [Regulation 2019/817¹¹](#), which is focused on information systems in the field of borders and visa, and [Regulation 2019/818¹²](#), on police and judicial cooperation, asylum and migration. On these grounds, a European search portal enables not only the comparison of fingerprints and facial images from several systems but also the discovery of identities associated to the same set of data.

The first question that arises is whether this automated research will upgrade the scrutiny in the migration process or be used as a panacea so as to avoid a personalised meticulous examination of each individual case, adapted to each person's special needs, characteristics, cultural background, age, sex and vulnerability. The results that occur from the search could be inaccurate. Nevertheless, since computers' outputs have an air of rationality or infallibility, people often blindly follow them either without questioning in good faith or attempt to minimise their own responsibility by following the computer's conclusion. The term "automation bias" is used to describe the inclination to trust computers (Borgesius,

¹⁰ [Directorate-General for Migration and Home Affairs](#) and [European Commission](#). Feasibility study of a Common Identity Repository (CIR) 2018-02-07.

¹¹ Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 OJ L 135, 22.5.2019, p. 27–84

¹² Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 OJ L 135, 22.5.2019, p. 85–135

2019) and it seems probable that it will challenge and weaken the chances of successfully opposing a decision, which was based on incorrect data. Effective legal remedies¹⁷ will meet the obstacle of the anonymity of the source of the information. In other words, states can use the interstate trust and not reveal the author of the information making it difficult to address justice and contest the decision.

The right to an effective remedy is protected by Article 47 EU Charter¹³ and Article 13 ECHR¹⁴. Nonetheless, fears have already been voiced about the new European Pact¹⁵, in which, rapid and efficient control over the borders seems to be ranked of higher importance than ensuring legal safeguards. According to the Pact, the authorities will be offered access to EU databases, in charge of the screening for the purpose of identity and security checks. Even if it is mentioned that there are only two possible outcomes of the screening, either asylum or return procedure, ECRE voiced the concern that they “*are in fact four possible outcomes: 1) refusal of entry, 2) return, 3) asylum, or 4) relocation.*” This means that there is the great **risk of refusal of entry without a procedure**¹⁶, since the person would merely be issued a debriefing form and be directly refused entry without the minimum the safeguards from the [Schengen Borders Code](#)¹⁷, such as having the right to appeal based on precise reasons of refusal (ECRE Policy Note#30 , 2020). The **absence of a written decision liable to appeal** and the **risk of refusal of entry without a procedure** cause great concerns. The only documents will be issued in a debriefing form and the person, who may wish to contest the decision, would not be guaranteed an appeal procedure open on referral¹⁸. We spot a possible violation of the rights of defense, if the person is not entitled being heard before the debriefing form is filled, as well as if he is not able to access the debriefing form in order to obtain reasons for the final decision (ECRE, 2020).

More specifically, when the screening process is completed, the authorities in charge would fill out a debriefing form containing personal and travel information¹⁹. Nevertheless, naming the document “de-briefing form” implies that it would not be regarded as an official decision. Indeed, the Regulation does not guarantee any rights of the individual to contest the

¹³ Charter Of Fundamental Rights Of The European Union 2012/C 326/02

¹⁴ Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocol No. 11 Rome, 4.XI.1950

¹⁵ European Commission New Pact on Migration and Asylum COM(2020) 609 final, 23 September 2020, 21–22.

¹⁶ Especially Article 14 of the Proposal for Screening Regulation raises this concern

¹⁷ Article 14 of the Schengen Borders Code (SBC), Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders

¹⁸ Articles 6(3), 6(4), and 6(5), Article 13 and 14(7), and Recital 19 of the Proposal for Screening Regulation

¹⁹ Article 13 of the Proposal for Screening Regulation

information included in the form. This lack in provision is notable, since this would be the only document issued at the end of the screening and it would contain information that could be proven crucial in both the referral and the procedure that follow. The European Commission justifies this absence of effective remedy on the grounds that in the subsequent procedure – return or asylum – the person would be able to submit the relevant decision to judicial review. In particular, Article 14(7) of the Proposal for Screening Regulation mentions that the screening would end when the person is referred to *return* or *asylum* procedure. Nevertheless, we have to underline that *the refusal of entry* procedure is not explicitly included in that provision. Hence, the lack of a possibility to review the de-briefing as regards people refused entry, is great since there is not procedure for them before a judicial authority. Some people would merely be issued a de-briefing form and be directly refused entry.

As the ECRE explains “*the proposal is to refuse entry on the basis of Article 14 SBC but without necessarily respecting the procedure laid down in that provision, including procedural safeguards*” (ECRE , 2020).

2.2. Collecting data from minors in registration procedures

In order to illustrate more vividly the impact of wrong assessment based on false data, we present the story (as broadcasted in a documentary by the Dutch radio-program [VPRO]) of a minor unaccompanied asylum seeker in Eurodac. The girl entered EU territory in Italy and was registered by the Italian authorities incorrectly into Eurodac as being an adult (E.Brouwer, 2019). Continuing her travel route north, she informed the immigration authorities in Netherlands (IND) of her actual age, 15 years old, and applied for asylum. Despite her claim of being minor and her obvious minor-appearance, the IND relied on the data submitted by the Italian authorities, supporting its denial to treat her as a minor on the principle of interstate trust. Even when she substantiated her age with documents, she did not receive the proper protection.

At this point it is important to stress the increased protection needs of all children who are not in the care of their parents or another adult responsible for their care (Network for the Rights of Moving Children, 2018). These "unaccompanied children" are in a vulnerable situation. The particular dangers to which they are exposed have been recognized by the European Parliament, which in a Resolution on the 25th anniversary of the United Nations

Convention on the Rights of the Child in November 2014,²⁰ emphasized that they are particularly vulnerable to abuse. The Parliament called on Member States to "take action to end the detention of migrant children across the EU". In the same European context, the EU Agency for Fundamental Rights (FRA), in a press release in September 2015, draws the attention of States to the urgent protection needed by children who arrive unaccompanied in the EU (European Union Agency for Fundamental Rights, 2015). The same organization in 2014 had published "A handbook on strengthening custody systems to meet the special needs of child victims of trafficking" (European Union Agency for Fundamental Rights, 2014), examining how existing systems respond to the special needs and vulnerabilities of child victims, or children who are at risk of marketing and exploitation, as in the case of unaccompanied ones (Dimitrova A, Penas DI, Ullam J., 2016). Additionally, in one ECHR case, that of Abdullahi Elmi and Aweys Abubakar v. Malta (2016)²¹, the court expressed its concerns in observation 103: "[Children] have special needs due in particular to their age and lack of independence but also to their status as asylum seekers. The [European] Court of Human Rights also recalls that the Convention on the Rights of the Child encourages States to take appropriate measures to ensure that a child seeking refugee status enjoys protection and humanitarian assistance, whether alone or accompanied by his parents (...)"

Moreover, it should be noted that, if in the end of the procedures which are used to verify the age of the child, there is still doubt, individuals enjoy the "benefit of doubt" and are treated as minors, until proven otherwise (Sarantou E, Theododopoulou A., 2019). Besides the child-unfriendly treatment and risk of re-traumatization occurring during data collection, the definition of age plays an important role: from the first moment of arrival, the rights- such as protection from returning to an unsafe country- and the entitled social benefits depend on the person's age.

The girl in our example, who was treated as an adult by the IND, did not receive proper child's protection, albeit she tried to prove her age with documents. Even if she had lied about her age to the Italian authorities, that was in fear of being separated from the group with which she entered Italy. Incorrect registration of age of minors is common practice: people under the age of 18 also pretend to be adults, in order to avoid protective measures that will prevent them from moving to their country of destination. There are even references to

²⁰ European Parliament resolution of 27 November 2014 on the 25th anniversary of the UN Convention on the Rights of the Child ([2014/2919\(RSP\)](#))

²¹ Case Of Abdullahi Elmi And Aweys Abubakar V. Malta (*Applications nos. [25794/13](#) and [28151/13](#)*) 22 November 2016 [FINAL](#) 22/02/2017

traffickers who specifically instruct young girls to declare that they are adults (Rights, 2018). The problems of children in registration procedures for immigration purposes are analysed in the report [Under watchful eyes](#) by the FRA (FRA, 2018). The same organization, in a 2017 [report](#), highlighted that, even if interoperability could service in finding missing children, this is possible only if Member States care more to report missing children into SIS II and improve cooperation between their national authorities (European Union Agency for Fundamental Rights, 2017).

The undoubtful conclusion is that incorrect information in even one of the databases has a high risk of being multiplied in other EU databases and at the national level. Focusing on children, there are proposals to enter in the databases the fingerprints of children as young as 6 years old and retain personal data for up to 5 years (in Eurodac, for up to 10 years) to facilitate deportation. However, FRA notices that *“taking the biometric data of very young children impacts on the quality and reliability of a future match. Fingerprints evolve over time, as the child grows.”* (FRA, Age assessment and fingerprinting of children in asylum procedures – Minimum age requirements concerning children’s rights in the EU, 2018). Fingerprint remaining stored for a decade increases the margin of error. Fingerprinting of children may influence a spectrum of fundamental rights, among these: the respect for human dignity, the right to physical and mental integrity and the right to information, or good administration. Specifically, if the procedure of fingerprinting is not carried out in a child-friendly manner, or if it is not executed by officials specifically trained in enrolling child fingerprints, the children’s dignity and physical integrity is affected. Additionally, when these fingerprints are stored and further processed in searchable IT systems the impact on human rights involves the personal data protection. The right to asylum, to liberty and security and the right to private life are directly dependent on the data evaluations. Still, there are challenges in correcting or deleting inaccurate data or unlawfully stored information, as well as there is risk of unlawful use and sharing of personal data with third parties. Having said that, we should keep under consideration that a child is in a weak position to exercise its right of access, correction and deletion of data. (FRA, Age assessment and fingerprinting of children in asylum procedures – Minimum age requirements concerning children’s rights in the EU, 2018).

2.3. The problem of compromised informed consent.

A child is in a weaker position to exercise its right of access, correction and deletion of data. The report [Digital Identity in the Migration and Refugee Context](#) confirms that through the identification process, migrants and refugees may be denied full safeguards of their privacy and data protection (Latonero, Hiatt, Napolitano, Clericetti, 2019). They are often offered only compromised informed consent, even if they are adults. For instance, adults refugees in Jordan have their irises scanned. Regretfully, [refugees in the Azraq camp have reported](#) (Staton B., 2016) deprivation of free and informed consent²², since in case they refuse the scanning, they are deprived from food (Molnar, 2019). It is clear that consent²³ is not free if it is provided under coercion. Authorities that create forced circumstances under the justification of efficiency or better service delivery violate migrants' human rights.

Hence, data may be initially collected with unlawful methods. Unlawful methods go in hand with lowered guarantees of quality; thus, the data may be inaccurate. Inaccurate data influence the decision-making procedure and result in fault decisions. Additionally, the complex system of databases hinder access to remedy, in case of abuse or error. These problematic aspects are violating the general principle of EU law, good administration, as at the same time they are violating- in a potentially irreversible manner- human rights' standards in EU's migration policy and longstanding approach to the data protection as a fundamental right (Ch. Jones, 2020). Regarding good administration, the European Charter of Fundamental Rights, provides in Article 41 the right to good administration, while Article 42 provides for the right of access to documents. The [Code of Good Administrative Behavior](#)²⁴ aims to detail and clarify the right, in order to avoid the maladministration by administrative bodies. Good administration is the process for issuing and executing administrative acts through procedures based on the rule of law. These procedures should be characterised by objectivity, fair, impartial and reasonable treatment, the right to be heard and make statements and indication of the possibilities of appeal (M. Batalli, A. Fejzullahu, 2018). Nevertheless, in migration-control procedures FRA has noticed that people "*lack awareness of data protection violations*

²² See also: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ (23 November 1995)

No L. 281 pp. 0031-0050

²³ The European Court of Human Rights has acknowledged that the protection of personal data, is of fundamental importance to the enjoyment of the right to respect for his or her private and family life guaranteed by Article 8 of the Convention (for example L.L. v. France (no. 7508/02))

²⁴ The European Code of Good Administrative Behaviour was proposed by the European Ombudsman and approved by the European parliament on 6 September 2001

and available remedies” (FRA, “Under watchful eyes – biometrics, EU IT-systems and fundamental rights”, 2018). Furthermore, if a person does consent, more likely he/she will also be deprived of information about their entry in a database, which makes it very difficult for her/him to exercise the right to access and rectify the data. Another aspect of good administration affected in instances of disrespectful conduct of border control and practices of compromised informed consent is the use of inappropriate language towards travelers. Language obstacles prevent effective communication and informed consent (FRA, “Fundamental rights at land borders: findings from selected European Union border crossing points Summary”, 2015).

In the next chapter, interoperability regulations are criticised for their discriminatory effects. Discrimination and data protection are interconnected since interoperable EU migration databases result in over-policing non-nationals only and it is lowering the protection of these groups’ personal data.

3. Protection of personal data and the discriminatory aspects of interoperability framework

A problematic aspect in the EU's new interoperability regulations relies in the notion that migration must be criminalized. The storage of personal and biometric data of every non-EU citizen who comes to Europe implies that serious crimes are mainly committed by foreigners and there is a need to prevent them. Nonetheless, people who come to EU to work, study or seek asylum are not more likely to commit crimes than EU citizens. Thus, the justification of these measures on combatting irregular migration and terrorism is not substantiated by relevant statistics and does not comply²⁵ with the principle of proportionality²⁶. Large-scale IT systems for immigration control and centralised databases come along with stigmatising migrants and strengthening punitive models to irregular migration (PICUM, How do the new EU regulations on interoperability lead to discriminatory policing?, 2020). It is discriminatory to target only non-EU nationals for purposes of anti-crime policies, because it pre-supposes and accepts a false connection between criminality and immigration.

²⁵ Article 5 European Union, *Treaty on European Union (Consolidated Version)*, *Treaty of Maastricht*, 7 February 1992, Official Journal of the European Communities C 325/5; 24 December 2002, available at: <https://www.refworld.org/docid/3ae6b39218.html>

²⁶ *Protocol (No 2) on the application of the principles of subsidiarity and proportionality* C 202/206, 7.6.2016, ELI: http://data.europa.eu/eli/treaty/tfeu_2016/pro_2/oj

There are not clear provisions on how data collection and processing of migrants complies with the requirements of lawfulness, necessity and proportionality. In the European Commission's landmark [White Paper on Artificial Intelligence: A European Approach to Excellence and Trust](#) it is explicitly mentioned that “*there must be a strict necessity for such processing (...) as well as appropriate safeguards. As any processing of biometric data for the purpose of uniquely identifying a natural person (...) AI can only be used for remote biometric identification purposes where such use is duly justified, proportionate and subject to adequate safeguards*” (European Commission, 19 February 2020).

The requirements of proportionality, respect for the right to data protection and appropriate safeguards are not met in the interoperability regulations, because there are not specific circumstances who justify such use, but rather there is the general suggestion that foreigners are engaged in activities threatening public security. There are weak anti-discrimination safeguards and a deficiency in circumscribing the exact offences that could give reason for access to the database (Ch. Jones, 2020).

More specifically, the new Migration Pact proposed procedures jeopardise ***data protection and privacy rights***²⁷. There are two main arguments that support this claim. First of all, besides consultation of the Common Identity Repository (CIR), there is an “expansion in purpose”, since data would be used for identification at the external borders, a purpose not initially mentioned in the Interoperability Regulation (ECRE Policy Note#30, 2020). The authorities will be offered access to EU interoperable databases, for the purpose of identity and security checks. Thus, there will be an expansion of the purposes and uses of EU information systems, which seems to aggravate data protection via lowering the safeguards. Expansions of the purposes of data processing and of the uses of EU information systems, including widening the range of actors granted access, sharpen long-standing concerns about the erosion of the *purpose limitation principle* and the protection of the right to private life, as well as the protection of personal data.

Secondly, the new procedures that are proposed in Migration Pact's, advance these identity checks to non-EU nationals²⁸. Random ID checks by the police to identify undocumented people are not rare in the EU. Nevertheless, allowing police officers direct access to information during random identity checks to non-EU nationals presents the risk of extensive use of databases and is not complying with the *strictly necessity test* (Molnar,

²⁷ Notably Articles 4(2), 9, 10 12, 13 14 and 14a of the amended Proposal for a Eurodac Regulation.

²⁸ Article 10, 11 13, 14 and 14a of the Proposal for a Regulation introducing a screening of third country nationals at the external borders.

2019). Assessing the necessity of data processing is demanded by the CJEU in *Digital Rights Ireland v. Ireland*²⁹ and in *Schrems v Data Protection Commissioner*³⁰, as well emphasised in the [EDPS toolkit](#) (European data protection Supervisor, 2017). For example, article 10(1)(b) of the Screening proposal would allow Member States to use 'data or information provided by or obtained from the third-country national concerned'. In other words, if there is difficulty in the identity verification processes, problematic practices such as making use of the information contained in migrants' smart phones, could be operated. Thus, the rights to data protection and privacy of third country nationals is seriously threatened. It would be more preferable and according to human rights protection standards that authorities continue to be able to see only the data that is relevant for the performance of their specific tasks and only via legitimate methods (European data protection Supervisor, 2017).

The EU Court of Justice has held that such checks should not be discriminatory, unnecessary or disproportionate³¹. However, the fact that interoperability and the centralization of data bases mainly affect third-country nationals fails to respect the fundamental right to non-discrimination. The EU Charter of Fundamental Rights guarantees to everyone the right to prohibition against discrimination (Article 21). Nevertheless, *“the new regulations, and the massive new information systems they create, only apply to non-EU nationals. They are based on the discriminatory and unfounded idea that migration and criminal justice are closely related and imply that serious crimes are only committed by foreigners. They reinforce a stigmatising and punitive approach to irregular migration.”* (PICUM, How do the new EU regulations on interoperability lead to discriminatory policing?, 2020). Direct discrimination, as defined in Article 2 (2) of the [EU Racial Equality Directive](#)³², is ‘taken to occur where one person is treated less favourably than another is, has been or would be treated in a comparable situation on grounds of racial or ethnic origin.’ In Migration’s Pact third-country nationals are treated less favourably, by comparison to how others in a similar situation would be treated; and the reason for this is a particular characteristic they hold, which is the migrant/ refugee profile. The criterion to determine if the border procedure will be uses is based on the nationality of the applicant. Nevertheless, the

²⁹ JUDGMENT OF THE COURT (Grand Chamber) 8 April 2014 *Digital Rights Ireland Ltd (C-293/12)*

³⁰ Judgment of the Court (Grand Chamber) of 6 October 2015. *Maximillian Schrems v Data Protection Commissioner*. Case C-362/14. ECLI identifier: ECLI:EU:C:2015:650

³¹ Case C 9/16 A v *Staatsanwaltschaft Oenburg* (2017) ECLI:EU:C:2017:483, Case C 278/12 PPU *Atiqullah Adil* (2012) ECLI:EU:C:2012:508, Joined cases C-188/10 and C-189/10 *Aziz Melki (C-188/10) C-188/10* and *Sélim Abdeli (C-189/10)* (2010) ECLI:EU:C:2010:363.

³² Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin

[Refugee Convention](#)³³ determines in Article 3 that “the Contracting States shall apply the provisions of this Convention to refugees without discrimination as to race, religion or country of origin”. Considering nationality as a decisive factor whether entry can or cannot be refused seems to contradict with this rule of international law.

3.1 Impact on migrant communities.

Regretfully, the Pact enhances *the risk of racial profiling*³⁴ and *delays* the start of the *asylum procedure*, even for those who visit the authorities voluntarily to apply for international protection (ECRE, 2020). In other words, not only those who are stopped in the borders, but also those stopped in the streets walking, as well those presenting themselves to the police in order to regulate their legal situation, no matter the differentiation of their cases, will be subjected to *screening within the territory*. This screening would ultimately channel those people to the return-or-asylum procedures.

The risk of ethnical profiling is highlighted by the fact that the burden of proof is reversed for the immigrants. In Article 5 of the Screening Proposal, we read that Member States '*shall apply the screening to persons found within the territory where there is no indication that they have crossed an external border to enter the territory of the Member States in an authorised manner*'. The application of this provision may give rise to discriminatory practices. Increased identity checks incite discrimination profiling and heightens migrant communities' feeling of being over-policed and under-protected. These people already face discriminatory policing and police harassment, as the EU recently recognized in the newly released [EU Action Plan Against Racism](#), which aimed “*countering discrimination by law enforcement authorities*” (Commission, 18.9.2020). Besides, the feeling of over-policing, these communities will be affected by the fact that the non-EU nationals, who are “found” or “apprehended” within the States’ territory will be facing detention. Experience of detention is linked to long-lasting negative impacts on people’s mental health and well-being (Red Cross EU , 2020). Migrants’ communities, which members face detention more often than other communities, are be severely affected.

Furthermore, there is another threat posed by not-fully-and properly -regulated use of technology regarding migrant communities. In addition to data for screening purposes, AI

³³ UN General Assembly, Convention Relating to the Status of Refugees, 28 July 1951, United Nations, Treaty Series, vol. 189, p. 137

³⁴ See Screening proposal, COM (2020) 612 final, Article 5

technologies are to be used in predictive policing. AI systems would use crime statistics to assess which individuals, neighborhoods and communities are more likely to commit crimes. However, the racial bias in existing policing approaches will result in inaccurate and discriminatory-inclined AI predictions (PICUM, Input To EU Consultation On Artificial Intelligence, June 2020). The sampling procedure is already biased. As it is noticed, *"If police focus attention on certain ethnic groups and certain neighbourhoods, it is likely that police records will systematically over-represent those groups and neighbourhoods"* (Lum K., Isaac W, 2016) . The present databases and available information will inevitably influence the programming and learning process of the AI. More specifically, since people with an immigrant background are stopped more by the police, police files over-represent migrants. Police register more crime in migrants' neighborhoods, thereby the effects of these biased samples would be intensified by AI predictions, which - based on the facts showing where more crime is registered- it will suggest that even more policemen are needed there. A vicious cycle of discriminatory over-policing tactics will be created. *"If biased data is used to train these predictive models, the models will reproduce (...) those same biases."* (Lum K., Isaac W, 2016) There will be increased policing in already over-policed city zones, triggering more arrests.

We have previously analyzed how, because of the black-box nature of AI algorithms, mistakes, inaccuracies, and biases are difficult to be detected (Beduschi A, 2020). Hence, contesting the legality of these arrests will possibly meet difficulty to obtain redress in case of violations of rights.

Conclusively, (1) police officers would use these technologies to detect whether individuals are present without authorisation. Thus, for those who are undocumented, the state's use of technology and processing of personal data will increase criminalization of their everyday life. The amplified use of digital technology intensifies policing of otherwise normal behaviors of marginalised people. On the other hand, (2) police AI systems will use biased samples and the implications of interoperability will be grave not only for undocumented, but documented people as well. It was argued above that the complexities of the interconnection of migration databases multiply the probability of errors, hamper information access on how data is used and how migrants can rectify their data, as well as how they and their lawyers could attain effective remedies in case of abuses. Besides these problematic consequences, we now analyzed how biometric surveillance technologies, AI systems and centralised interoperable databases, disproportionately affect minority ethnic communities.

Sarah Chander, Senior Policy Advisor at [European Digital Rights](#)³⁵ explains how these technologies discriminate against “*racialised communities, LGBTIQ+ people, people with disabilities, workers, undocumented migrants, sex workers, and the organisations representing their rights.*”, because there are “*(...) countless examples of how AI systems can be used to harm people and society – from enabling biometric mass surveillance to exacerbating discrimination to the extraction of data from migrants in vulnerable situations.*” (Chander, 2021). In the following sub-chapter, we will examine a specific use of AI, in order to illustrate more accurately some of its possible harmful effects to migrant’s communities.

3.2. Non-discrimination principle and AI: the facial recognition example and biased sample

A cornerstone of biometric surveillance technologies is facial recognition. U.S. National Institute of Standards and Technology (NIST) found that facial recognition systems are remarkably more likely to result to incorrect positives among people of colour (NIST, 2019). Nonetheless, facial recognition is applied in immigration enforcement. According to European Data Rights (EDRI), “*at least 15 European countries have experimented with highly intrusive facial and biometric recognition systems for mass surveillance*” (EDRi, 2021).

Facial recognition can be used not only for identification, but also as a lie detector or an emotion recognition system. Assessing whether a refugee’s life story is ‘truthful’, whether an immigrant’s marriage is ‘genuine’ presupposes that all peoples’ credibility can be measured by AI systems according to limited criteria (Satzewich, 2014). However, constituting truthfulness standards is highly difficult, given the differences in cross-cultural communication. Bias in identification has already been reported in facial recognition (FRA, Facial recognition technology: fundamental rights considerations in the context of law enforcement , 2019) technologies, who seem to error in analyzing women or people with darker skin tones and evaluating their emotional reactions. Humans do not experience or express reality in the same way. Thus, migration stories cannot easily be limited to an algorithm (Ch. Jones, 2020). Likewise, AI are not perfect and dealing with trauma is a complex process even for doctors. It is proven that trauma has an effect on memory (Program for the Rehabilitation of Survivors of Torture , 2017). Additionally, memory is personal and

³⁵ European Digital Rights (EDRi) is an association of civil and human rights organisations from across Europe.

trauma is a psychological element. Extracting the “truth” via AI facial recognition programs raises concerns about information sharing without people’s consent.

Since we have previously focused on children, we should highlight that the child’s best interests ³⁶ must be given a primary consideration in the context of using facial recognition. A stricter necessity and proportionality test is needed, because of the particular vulnerability of children. Similarly, to fingerprints, the risk of a wrong match increases when facial images are recorded at a young age (PICUM, Input To EU Consultation On Artificial Intelligence, June 2020). Additionally, the expression of migration experience is not the same in minors as in adults and AI systems may find difficulties to assess children’s statements and reactions.

Conclusively, while AI may accelerate decisions, it may as well deter their quality and aggravate access to justice (EDRI, 2020). The nuanced nature of immigration issues is incompatible with massive evaluations, many of which are formed with bias, under discriminatory notions, in ways that violate privacy, due process and procedural fairness. The personalized claims of migrants may be misinterpreted, causing breaches of human rights. Algorithmically driven identification technologies disproportionately mis-identify people from minority ethnic groups. Moreover, predictive policing systems are pre-disposed to depict geographic areas with a high proportion of minority ethnic people as criminally-inclined. This bias is drawing even more police attention and provokes grave personal and emotional unrest to the people living there, who feel that they are being discriminated against (Williams P. , Kind E., 2019). The collection of extensive information about individuals and their associations in these communities, deprives them from privacy and breaches the presumption of innocence. Racialised criminalization affects not only the understandings of crime, but also the design of anticrime policies, thus there is a domino effect.

3.3 AI’s possible repercussions in collective and individual enjoyment of migrants’ human rights.

The AI crucial complications for ordinary people with migrant background concern a wide spectrum of their rights: the right to equality and non-discrimination; freedom of movement, expression, religion, and association; privacy rights and the rights to liberty and security of the person.

³⁶ United Nations Convention on the Rights of the Child, New York, 20 November 1989 (1577 U.N.T.S., p. 3).

The right to equality and non-discrimination (Art. 21 Eu Charter) is mainly affected by biased samples in the AI programs, as well as racial profiling, aspects we discussed in detail. If a system is fed with human prejudices the result will inevitably be influenced. *“There is increasing evidence that women, ethnic minorities, people with disabilities and LGBTI persons particularly suffer from discrimination by biased algorithms”* (Mijatović, 2018). Consequently, instead of making migration-related decisions fairer, AI could reinforce discrimination and prejudices in a façade of objectivity. Additionally, *“the increasingly fervent collection of data on migrant populations – so-called data colonialism – can also result in privacy breaches and raise human rights concerns”* (Molnar, 2019). However, other fundamental human rights are also affected and we will examine AI’s impact on them briefly, but carefully.

The freedom of movement (Art. 45 EU Charter) is violated, for example, if AI wrongful decisions end in wrongful deportations, such as the deportation of over [7,000 foreign students from the UK](#), after AI systems had incorrectly concluded they had cheated on a language acquisition test. As far as liberty is considered, false AI estimations that would lead to detention, would have grave consequences to migrant’s physical, psychological integrity and dignity, as well as it will probably cause prolonged family separation. AI’s connection to amplified use of detention gained more attention in June 2018, when US Immigration and Customs Enforcement (ICE) was accused of using an algorithm that primarily recommended the [detention of migrants](#) to comply with the policies on the US-Mexico border. It is important to keep in mind that, while detention should be a measure of last resort, the New European Pact does not oblige States to prioritise alternatives to detention (Red Cross EU , 2020).

The freedom of expression (Art. 11 EU Charter of Fundamental Rights) is exposed to a serious backsliding of AI, which is the restriction of migrants’ free expression online, in social media, for fear of having their opinions used later against them. The Council of Europe has noted in its [publication on Algorithms and Human Rights](#) that Facebook and YouTube have put into practice a filtering mechanism that detects “violent extremist content”. Nonetheless, there is lack of transparency, because no information is available as regards the process and criteria that lead to banning some online content as “clearly illegal”. Therefore, it is likely that the mechanism is used to restrict legitimate free speech and to infringe on people’s expression. Migrants may not post online their thoughts, fearing they would be

labeled “extremists” and they would not be allowed to enter or to stay in the country in which they seek a better future. Thus, AI could mean self-censor or internet-censor.

Moreover, codifying (intentionally or because of biased sample in the algorithms) believers of a particular religion (ex. Islam) as possible “terrorists” will restrict the right of religion (Art.10 EU Charter). AI could assist government officials in monitoring and targeting members of certain religious groups. Migrants may be hesitant to display religious symbols online. These are not ungrounded fears. For instance, German migration authority already uses mobile phone extraction technology in the asylum application procedure. A [German NGO](#) underlines that contacts, call data, text messages, stored files, location information, and more are extracted “*regardless of any concrete suspicion that the asylum-seekers made untruthful statements regarding their identity or country of origin*” (Biselli A., Beckmann L., 2020). German is just one example out of many. All asylum seekers in Norway are asked by police to provide their phones and Facebook login details (Brekke J.-P., Staver A.B., 2019). Even if governments assure migrants that they are interested in specific data and not their personal beliefs, migrants would feel supervised. Anyone who feel under surveillance, alter his/her behavior and become less spontaneous, more cautious. Migrants feeling this way, may adapt their online profiles so as they seem “good/accepted European citizens”, even this means self-restriction and abstention of expressing their religion and thoughts. Weaponising migrants’ phone against them has long-reaching consequences for human rights’ protection and it is violating the proportionality and necessity test.

In addition, understanding the internet as a collective space where human rights are exercised, we recognise that many vulnerable groups and individuals, among them migrants- especially those deprived of liberty- use the internet as the sole space in which they can exercise their human rights, including the right to assembly and association (Art. 12 EU Charter of Fundamental Rights). UN Special Rapporteur on the rights to freedom of peaceful assembly and of association stated in his 2019 report that he “*is concerned about the variety of measures and tactics that are used by States to control and impede access to and use of digital technology for the exercise of the rights to freedom of assembly and of association*” (Voule, 2019). Likewise, in the Freedom of association for migrants [Joint statement](#) at Human Rights Council it was noted that “*defenders of migrants’ and refugee rights play a crucial role in supporting migrants, elevating their voices and providing humanitarian assistance. We are seriously alarmed at the harassment of individuals and civil society organizations supporting migrants, including migrant workers, in the EU and the US;*

including criminalization of their activities; and barriers to registration and funding. Such attacks can be a matter of life or death for those whose rights and freedoms they defend.” (Joint statement at Human Rights Council, 2020).

Privacy rights (Article 8 EU Charter of Fundamental Right) are threatened since there is no guarantee that migrants-data subjects will be able to refuse having their data shared, as well as whether they will have access to a fair mechanism for claims and appeals that will ensure accountability and transparency (PICUM, Data protection and the “firewall”: advancing the right to health for people in an irregular situation platform for international cooperation on undocumented migrants, 2020).

Furthermore, as we analysed in detail on previous chapters, the use of such technologies in the migration system touches constitutional and administrative law issues, as well as it downgrades access to justice, and public confidence in the legal system (International Human Rights Program and the Citizen Lab , 2018). The right to an effective remedy before a tribunal and to a fair trial (Article 47 of the Charter) is of vital importance and data processed by AI-driven technologies should fall under no exception from this safeguard.

In the following chapter, we will examine how technology (if not properly regulated) could increase not only discrimination, but also exclusion of some groups, especially, communities of colour (PICUM, Input To EU Consultation On Artificial Intelligence, June 2020). More specifically, we will analyse how AI may undermine ‘firewalls’ between public services and immigration enforcement. In other words, we will examine AI’s impact on social rights.

4. ‘Firewalls’ between public services and immigration enforcement and the issue of accountability

Migrants may be reluctant to address the authorities or social services, fearing that their personal data collected in these services, will later be used against them. This fear would limit their access to hospitals, police and social services. It is advisable to implement “firewalls” that prevent the processing of data of a victim or witness to promote access to justice (PICUM, Input To EU Consultation On Artificial Intelligence, June 2020). Reporting crimes is in benefit of the public good and community safety. Eradication of illness is also vital- and the COVID-19 pandemic proved it: actual and effective protection of public health means

access to hospitals for all, citizens and non-citizens. Data collected in health and social services cannot be used to file for the deportation of the individual, because the data collected under these circumstances are usually sensitive (revealing racial or ethnic origin, concerning health or sexual orientation), thus entitled enhanced protection according to the GDPR³⁷. Therefore, these data should be used for the purpose that are strictly collected for (PICUM, Data protection and the “firewall”: advancing the right to health for people in an irregular situation platform for international cooperation on undocumented migrants, 2020). Misuse of data is a risk which addresses the heart or ‘essence’ of the right to private life and data protection, protected in Article 8 ECHR and 7³⁸, respectively 8 of the Charter³⁹ on Fundamental Rights (E.Brouwer, 2019).

Over-zealous use of these data, meaning extracting them for migration checks, will perpetuate discrimination and social exclusion. Furthermore, [EDPS in Opinion 4/2018](#) comments that interoperability regulations, creating new centralised databases containing information on millions third-country nationals, pose the risk that if *‘such information ever falls into the wrong hands, the database could become a dangerous tool against fundamental rights’*. Unrestricted or disproportional processing and use of personal information has already been addressed in both the CJEU and the ECtHR. In [S. and Marper v. UK](#),⁴⁰ ECHR acknowledged that storing information on large groups of unsuspected people into centralised databases for law enforcement purposes poses the risk of stigmatization. CJEU found that data processing involving persons without any link to criminal prosecution breaches the right to privacy and data protection⁴¹. Given that under the interoperability framework national powers will be able to check a vast number of individuals not only at the borders, but also within the national territory, the Courts’ rulings are to be beared in mind.

We shall not underestimate the problem of transparency of powers. Recent reports (M. Douo, L. Izuzquiza, M. Silva, 2021) expose Frontex holding special events with security industry lobbyists, who represent corporate interests and are not neutral parties. The report

³⁷ European Parliament and Council of European Union (2016) Regulation (EU) 2016/679. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>.

³⁸ Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocol No. 11 Rome, 4.XI.1950

³⁹ Article 8 EU Charter of Fundamental Rights Official Journal of the European Union C 303/17 - 14.12.2007.

⁴⁰ *S. and Marper v. United Kingdom*, Applications nos. 30562/04 and 30566/04, Council of Europe: European Court of Human Rights, 4 December 2008, available at:

<https://www.refworld.org/cases,ECHR,4ee21cbe2.html> [accessed 21 February 2021]

⁴¹ JUDGMENT OF THE COURT (Grand Chamber) 8 April 2014 Digital Rights Ireland Ltd (C-293/12)

alerted that FRONTEX has no real transparency or lobbying accountability mechanisms in place.

As far as the new European Pact⁴² on Migration and Asylum proposals are concerned, Frontex and EASO will have power over many processes, influencing each individual decision making in a legal landscape of accountability gap, since their role and competencies are not yet clearly defined (ECRE, 2020). It has been argued that the *“new procedural steps introduced by the Pact such as the screening at the external borders or the border procedure, neither take to account the particularities of the potential involvement of EU agencies in these processes nor do they frame these executive powers. This could have a potential impact on migrants’ procedural rights (...) This could potentially impact the effectiveness of administrative cooperation and migrants’ fundamental rights protection.”* This argument stands on the fact that *“operational support under this framework will not be covered by the enhanced fundamental rights protection layer that has been developed by FRONTEX including, among other, a fundamental rights officer, an individual complaints mechanism, and fundamental rights monitors.”* (Tsourdi, 2020). We spot a deficiency of legal aid and accessible information in the pre-entry screening procedures and inadequate provisions in order to appeal against negative decisions.

It is essential to establish effective oversight and accountability mechanisms to keep FRONTEX under actual democratic control. The expansion of FRONTEX in an accountability vacuum will mean that the security industry lobbies will de-facto shape EU’s approach to border control in their interests. FRONTEX does not demand surveillance companies to provide their EU Transparency Register number; neither do they invite in their meetings any human rights organization, regardless of the impact of these technologies and products on human rights. There is only a consultative forum on human rights that is rarely been consulted. Additionally, there is no system of transparency, where meetings with third-party stakeholders are registered, even if FRONTEX had committed *“to develop the policy and a fully-fledged system by beginning of 2021 the latest”* (Statewatch, 2020).

Transparency is a demand even more urgent, fair and necessary after the interoperability regulations, since they add to the complexity of practices and augment applied guidelines. Each new instrument in charge of data processing has its set of data protection rules, something that according to EDPS’s [Opinion 4/2018](#) produces an unclear legal framework,

⁴² European Commission New Pact on Migration and Asylum COM(2020) 609 final, 23 September 2020, 21–22.

adding to the general rules of the [GDPR](#)⁴³ and the [Data Protection Directive](#). Lack of simplicity in the legal regime results in uncertain accountability and liability when incorrect or unlawful data processing is revealed. As the number of databases and the users involved increases, the harder it gets for the subject to be aware of the particular law that applies and the state or organization that should be addressed.

European Commission has recognized that it may even be difficult to diagnose that an unlawful practice has been made: *“Enforcement authorities and affected persons might lack the means to verify how a given decision made with the involvement of AI was taken and, therefore, whether the relevant rules were respected”* (European Commission, 19 February 2020). Given that understanding whether the law was followed meets obstacles, then the difficulties in proving such an infringement are obvious. The Commission has also acknowledged that *“individuals and legal entities may face difficulties with effective access to justice in situations where such decisions may negatively affect them.”*

As for the individuals, their access, correction or deletion of data, and their right to effective judicial protection seem more puzzling than ever before. On the other hand, if authorities have access to personal data, without consent or beyond accountability, transparency is challenged.

5. Legal framework and recommendations

While AI innovations have been flourishing in the last years, it is inaccurate to believe that they are developing in a legal vacuum. States are still internationally obligated to respect human rights under a number of conventions, especially the International Covenant on Civil and Political Rights⁴⁴, the International Covenant on Economic, Social and Cultural Rights⁴⁵. Even in the absence of a *lex specialis* for all AI uses, all policies are anticipated to provide remedy and redress for human impacts caused by AI (Desierto, 2020) .

The EU Charter of Fundamental Rights⁴⁶ guarantees to everyone the right to: Respect of privacy and family life (Article 7); The protection of their personal data (Article 8);

⁴³ Ibid Regulation (EU) 2016/679 GDPR n(67)

⁴⁴ The United Nations General Assembly. 1966. “International Covenant on Civil and Political Rights.” Treaty Series 999 (December): 171.

⁴⁵ The United Nations General Assembly. 1966. “International Covenant on Economic, Social, and Cultural Rights.” Treaty Series 999 (December): 171.

⁴⁶ European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02, available at: <https://www.refworld.org/docid/3ae6b3b70.html> [accessed 21 February 2021]

Prohibition against discrimination (Article 21); Fair administration (Article 41) and to an effective remedy (Article 47) when rights are violated.

The European Convention on Human Rights⁴⁷, of which all EU countries are a party, guarantees the right to respect private and family life (Article 8).

The Committee on Economic, Social, and Cultural Rights, on its [General Comment No. 24](#), has laid emphasis on the State's duties to take steps to regulate business activities that may adversely affect economic, social, and cultural rights, particularly to avoid worker, migrant, sexual, religious, racial or other forms of *discrimination* (UN Committee on Economic, Social and Cultural Rights (CESCR), 2017,). AI products that are used for border and migrations processes fall under these duties. The Committee also called States parties' attention to the fact that "*obligations under the Covenant did not stop at their territorial borders. States parties were required to take the steps necessary to prevent human rights violations abroad by corporations domiciled in their territory and/or jurisdiction (whether they were incorporated under their laws, or had their statutory seat, central administration or principal place of business on the national territory), without infringing the sovereignty or diminishing the obligations of the host States under the Covenant.*"

On the same page, the European Union is working towards ensuring the meaningful, informed, and free consent of individuals, as mentioned in its [2019 Ethics Guidelines for Trustworthy Artificial Intelligence](#). The Guidelines set seven key requirements for trustworthiness of AI systems: 1) human agency and oversight (including fostering informed decisions respectful of individual human rights); 2) technical robustness and safety; 3) privacy and data governance; 4) transparency; 5) diversity, non-discrimination, and fairness; 6) societal and environmental well-being; and 7) accountability (Report from the Commission, 2019).

The European Commission is aware that the specific and complex characteristics of AI technologies, ('black box-effect') may make it challenging to "*verify compliance with, and may hamper the effective enforcement of, rules of existing EU law meant to protect fundamental rights.*"⁴⁸ The European Commission aims to address the problems of AI, wishing to "*EU's technological leadership and to ensuring that new technologies are at the service of all Europeans – improving their lives while respecting their rights*". Hence, it

⁴⁷ Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5, available at: <https://www.refworld.org/docid/3ae6b3b04.html> [accessed 21 February 2021]

⁴⁸ Ibid European Commission n(78)

proposes a common European approach to AI grounded in EU's values and fundamental rights such as human dignity and privacy protection.

The proposed common European approach is a **risk-based approach**, so that the regulatory intervention is proportionate. It is mentioned that *“the use of AI applications for the purposes of remote **biometric identification** and other intrusive surveillance technologies, would always be considered “high-risk” and therefore the below requirements would at all times apply”*. Regardless of the risk, the Commission suggests taking reasonable measures aimed at ensuring that AI systems are robust and accurate and *“does not lead to outcomes entailing prohibited **discrimination**”*. In order to achieve this objective, the Commission recommends human oversight, because *“ethical and human-centric AI can only be achieved by ensuring an appropriate involvement by human beings in relation to high-risk AI applications”*. Moreover, transparency *“is required also beyond the record-keeping– in particular promoting the responsible use of AI, building trust and facilitating redress where needed”*.

The Commission proposals are in agreement with the EU General Data Protection Regulation (GDPR), which applies to everyone in the EU whose data is processed (Article 1) and requires transparency and accountability in the processing of personal data (Article 5). This Regulation grants specific data subject rights (Articles 12 to 22), among which the right to information and the right of access, rectification and erasure. The GDPR⁴⁹ prohibits the profiling of individuals through automated processing (Article 22) and requires the existence of independent national supervisory authorities that shall inform people of their rights and help them to access justice when their rights are violated.

GDPR sets three principals that are of great importance and relevance regarding surveillance technologies in migration processes. Firstly, it highlights the “purpose limitation”⁵⁰ by setting strict limits on the reasons for which data can be processed. Personal data cannot be collected, except for specified, explicit and legitimate purposes. Thus, data collected for one purpose shall not be further processed in incompatible ways with this purpose (PICUM, Data protection and the “firewall”: advancing the right to health for people in an irregular situation platform for international cooperation on undocumented migrants, 2020). Secondly, the GDPR prohibits processing of personal data beyond what is strictly

⁴⁹ Ibid GDPR n(67)

⁵⁰ Ibid GDPR n(67) Article 5

needed to achieve the purpose for which the data was initially collected, a restriction called “data minimization”. Thirdly, the GDPR provides enhanced protection for sensitive data.

There is only thin margin for exceptions. Exceptions to the GDPR are narrow, because data protection and privacy rights are fundamental rights. Any deviation from the GDPR should be grounded on transparent EU or national legislation that is in (a) full respect with the fundamental rights and freedoms of individuals who would be affected and are acceptable only if (b) it safeguards a specific and pressing social need, (c) is sufficiently clear and precise to be foreseeable to affected individuals; and (d) is necessary and proportionate in a democratic society.

The European interoperability initiative contains regulations that are incompatible with GDPR, especially **purpose limitation**. Opening the door for facilitating identity checks via the CIR, migrants’ data will be subject to large-scale, automated cross-checking through the Multiple Identity Detector (MID⁵¹). Nevertheless, the existing databases were established for particular purposes. To be more specific the VIS was launched for the issuing of short-stay Schengen visas⁵², while the EES was founded for the registration of crossings of the external Schengen borders⁵³. The use of data for new purposes, were never stated in the original lawmaking violated the principle of purpose limitation (Jones, 2019).

Until today, checking of migrants’ data was based on the central Eurodac database, with the fundamental difference that these data were not stored. According to the proposed changes, data will be stored in Eurodac and added to the CIR. Many and main fundamental rights could be affected by the current proposals. Namely, we previously analysed impacts on the right to asylum (Article 18 EU Charter), the prohibition of torture and inhuman or degrading treatment or punishment (Article 4 EU Charter, Article 3 ECHR), while we discussed why AI incorrect decision may lead to denial of liberty or detention, which is related to the right to liberty and security (Article 6 EU Charter, Article 5 ECHR), the protection in the event of removal, expulsion or extradition (Article 19 EU Charter) and the right to an effective remedy (Article 47 EU Charter, Article 13 ECHR) (ECRE Comments, 2020).

⁵¹ Brussels, 12.12.2017 COM(2017) 794 final 2017/0352 (COD) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) 474 final}

⁵² European Commission- Migration Affairs- Visa Information System (VIS) Brussels, 17.12.2020 C(2020) 8000 final 17.12.2020

⁵³ Brussels, 6.4.2016 Accompanying Regulation (EC) No 767/2008 and Regulation (EU), No 1077/2011 and Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) {SWD(2016)

Beyond those, the rights of the child (Article 24 EU Charter) would be menaced by the expansion of migration-related surveillance and identification methods. Even if all EU Member States have ratified [Convention on the Rights of a Child](#) which prioritise the best interest of the child, the Commission new Pact on Migration lowers the protection standards for children. Contrary to the global definition of children as “every human being below the age of eighteen years” (Art.1 of Convention on the Rights of a Child), the Pact⁵⁴ suggests that only children younger than 12 years old should be protected from some harmful border procedures. “*Children aged 12-18 who are accompanied by their parents or other caregivers are required to undertake the border procedures, which translate into almost automatic detention and lack of access to regular pathways beyond asylum.*” (PICUM, More detention, fewer safeguards: How the new EU Pact on Migration and Asylum creates new loopholes to ignore human rights obligations, 2020). Allowing children’s detention for potentially up to 10 months infringes international and regional [standards](#), as those set by the Committee on the Protection of the Rights of All Migrant Workers and Members of Their Families,⁵⁵ that denounce child immigration detention as a violation of the rights of the child. The best interest of the child shall be a primary consideration and it would be regretful if the Commission was to lower the protection standards for children.

NGOS, civil society and activists have urged international, European, national and city-level authorities to rethink and reform their approach to migration. PICUM has issued specific recommendations, urging to “*move towards proportionate, humane and sustainable migration policies*” that would put an end on discrimination and inequalities based on class and race. Among these recommendations, PICUM advocates in favour of “firewalls” to safeguard that personal data acquired when undocumented people access health care or social services, or report crime, are not repurposed for immigration control. PICUM also calls for a review of the implications for “*communities of colour, and other at-risk groups, of the use of technology in predictive policing and immigration control*” and for “*clear guidelines about policing and the use of personal data and algorithms, based on meaningful input from and engagement with relevant stakeholders*” (Ch. Jones, 2020). Lastly, we underline PICUM’s

⁵⁴ Article 41 (5) AMENDED PROPOSAL FOR AN ASYLUM PROCEDURES REGULATION COM(2020) 611

⁵⁵ UN Committee on the Protection of the Rights of All Migrant Workers and Members of Their Families (CMW), *Joint general comment No. 4 (2017) of the Committee on the Protection of the Rights of All Migrant Workers and Members of Their Families and No. 23 (2017) of the Committee on the Rights of the Child on State obligations regarding the human rights of children in the context of international migration in countries of origin, transit, destination and return*, 16 November 2017, CMW/C/GC/4-CRC/C/GC/23

appeal for enhanced accountability “*for the implications of digital technology and data processing for human rights and discrimination*” (Ch. Jones, 2020).

6. Conclusion

Technology advances faster than ethics are coded to laws. A sharper human-right’s-based oversight on mechanisms is required. This study revealed that data-driven policing solutions are neither objective, nor unflawed. We have to unmask the lack of accountability that lies under the neutrality belief: predictive policing programs *can* be biased; algorithm evaluations *can* be wrong.

Therefore, strict provisions shall determine who and when should have access to the migrants’ data. Structural discrimination should be avoided, thus migrants’ data obtained in social services should not be later used for immigration control. Additionally, ensuring accountability is needed in order to minimize the implications of digital technology and data processing for human rights and discrimination.

It was highlighted why the European Union's response to migrants should be driven by the protection of human rights. Difficult times require more commitment to our values, not eluding responsibilities (Joint Statement ECRE, 2020). Many recent proposals about migration policy cannot be adopted in their current form, without violating- in a potentially irreversible manner- human rights’ standards in EU’s migration policy.

These recommendations are articulated based on the belief that border protection should not be shaped by the interests of defense companies instrumentalising migration for profit. We hope and urge the EU to point towards maintaining and raising asylum and human rights standards in Europe, rather than amplifying returns, expanding detention and lowering privacy standards (PICUM, Input To EU Consultation On Artificial Intelligence, June 2020). For that reason, instead of multiplying the exemptions to human rights protection on the surveillance area, EU could review the AI plans, guaranteeing democratic oversight, systems of accountability, safeguarding freedom from discrimination and privacy rights. At present, new technologies in migration are largely unregulated. EU can work in the direction of establishing procedural justice safeguards, such as the right to a fair decision-making process and the right of appeal.

To put it in a nutshell, technology is a tool that could serve humanitarian goals at the same time as it could benefit states' and EU's interests. For instance, AI could be used for preventing arrivals and increasing deportations (Beduschi A, 2020), but equally it could assist states and international organisations in preparing for large movements of people, via predicting flows or helping in allocating resources. If EU stays truthful to its founding principles, it may lead the path globally in seeking to ensure fair and beneficial use of technology for migration policy purposes.

Bibliography

- Batalli M, Fejzullahu A. (2018). Principles of Good Administration under the European Code of Good Administrative Behavior. *Pécs Journal of International and European Law* , pp. 26-35.
- Beduschi A. (2020, February 10). International migration management in the age of artificial intelligence. *Migration Studies*(ms.3). Ανάκτηση από <https://academic.oup.com/migration/advance-article/doi/10.1093/migration/mnaa003/5732839>
- Biselli A., Beckmann L. (2020). Invading Refugees' Phones: Digital Forms of Migration Control . *Gesellschaft für Freiheitsrechte / Society for Civil Rights*.
- Brekke J.-P., Staver A.B. (2019, June). Social media screening: Norway's asylum system. *Ethics*(61).
- Borgesius, F. Z. (2019, February 7). *Discrimination, Artificial Intelligence and Algorithmic Decision-Making*. doi:[https://www.coe.int/en/web/artificial-intelligence/-/news-of-the-european-commission-against-racism-and-intolerance-ecri-](https://www.coe.int/en/web/artificial-intelligence/-/news-of-the-european-commission-against-racism-and-intolerance-ecri)
- Chander, S. (2021, March 16). *This is the EU's chance to stop racism in artificial intelligence*. Ανάκτηση από EDRi : <https://edri.org/our-work/this-is-the-eus-chance-to-stop-racism-in-ai/>
- Commission, E. (18.9.2020). *EU anti-racism action plan 2020-2025*. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions a Union of equality : , Brussels. Ανάκτηση από https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-anti-racism-action-plan-2020-2025_en
- Desierto, D. (2020, February 26). *Human Rights in the Era of Automation and Artificial Intelligence* . Ανάκτηση από Blog of the European Journal of International Law: <https://www.ejiltalk.org/human-rights-in-the-era-of-automation-and-artificial-intelligence/>

- Dimitrova A, Penas DI, Ullam J. (2016, January 20). *Unaccompanied Migrant Children In The EU*. Ανάκτηση από European Parliamentary Research Service Blog:: <https://epthinktank.eu/2016/01/20/unaccompanied-migrant-children-in-the-eu/>
- E.Brouwer. (2019, May 14). *Interoperability and Interstate Trust: a Perilous Combination for Fundamental Rights*. Ανάκτηση από EU Immigration and Asylum Law and Policy: <https://eumigrationlawblog.eu/interoperability-and-interstate-trust-a-perilous-combination-for-fundamental-rights/>
- ECRE Policy Note#30 (2020). *Screening out rights? Delays, Detention, Data concerns and the EU's Proposal for a Pre-entry Screening process*. Ανάκτηση από Retrieved from European Council on Refugees and Exiles: <https://www.ecre.org/ecre-policy-note-screening-out-rights-delays-detention-data-concerns-and-the-eus-proposal-for-a-pre-entry-screening-process/>
- ECRE . (2020, October 18). *ECRE Comments: on the Commission Proposal for a Screening Regulation COM (2020) 612*. Ανάκτηση από European Council on Refugees and Exiles: <https://www.ecre.org/ecre-comments-on-the-commission-proposal-for-a-screening-regulation-com-2020-612/>
- ECRE. (2020). *ECRE Comments: on the Commission Proposal for a Screening Regulation COM (2020)* . Retrieved from European Council on Refugees and Exiles .
- ECRE Comments. (2020, December 18). *On the Commission Amended Proposal for an Asylum Procedures Regulation COM (2020) 611 Border Asylum Procedures and Border Return Procedures*. Ανάκτηση από European Council on Refugees and Exiles: <https://www.ecre.org/ecre-comments-on-the-commission-amended-proposal-for-an-asylum-procedures-regulation-com-2020-611-border-asylum-procedures-and-border-return-procedures/>
- ECRE Policy Note#29. (2020, December 18). *Relying on a Fiction: New Amendments to the Asylum Procedures Regulation*. Ανάκτηση από European Council on Refugees and Exiles: <https://www.ecre.org/wp-content/uploads/2020/12/Policy-Note-29.pdf>
- ECRE Policy Note#30. (2020, December). *Screening out rights? Delays, Detention, Data concerns and the EU's Proposal for a Pre-entry Screening process*. Ανάκτηση από European Council on Refugees and Exiles: <https://www.ecre.org/wp-content/uploads/2020/12/Policy-Note-30.pdf>

- EDRI. (2020, February 12). *The human rights impacts of migration control technologies* .
Ανάκτηση από EDRI : <https://edri.org/our-work/the-human-rights-impacts-of-migration-control-technologies/>
- EDRI. (2021, May 13). *Ban biometric mass surveillance!* Ανάκτηση από EDRI :
<https://edri.org/our-work/blog-ban-biometric-mass-surveillance/>
- European Commission. (19 February 2020). *White Paper on Artificial Intelligence: a European approach to excellence and trust* . COM(2020) 65 final.
- European data protection Supervisor. (2017, April 11). *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*.
Ανάκτηση από https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en
- European Union Agency for Fundamental Rights. (2014, June 30). Guardianship for children deprived of parental care. Ανάκτηση από
<https://fra.europa.eu/en/publication/2014/guardianship-children-deprived-parental-care>
- European Union Agency for Fundamental Rights. (2015, October 16). Guardianship systems for children deprived of parental care in the European Union. Ανάκτηση από
https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-guardianship-systems-in-the-eu_en.pdf
- European Union Agency for Fundamental Rights. (2017, May). *Fundamental rights and the interoperability of EU information systems: borders and security* , . Ανάκτηση από
<https://fra.europa.eu/en/publication/2017/fundamental-rights-and-interoperability-eu-information-systems-borders-and-security>
- FRA. (2018, April 25). *Age assessment and fingerprinting of children in asylum procedures – Minimum age requirements concerning children’s rights in the EU*. Ανάκτηση από
European Union Agency for Fundamental Rights:
<https://fra.europa.eu/en/publication/2018/age-assessment-and-fingerprinting-children-asylum-procedures-minimum-age>
- FRA. (2019, November 27). *Facial recognition technology: fundamental rights considerations in the context of law enforcement* . Ανάκτηση από European Union Agency for Fundamental Rights: <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law>

- FRA. (2015). *Fundamental rights at land borders: findings from selected European Union border crossing points Summary*. European Union Agency for Fundamental Rights.
- FRA. (2018, March 28). *Under watchful eyes – biometrics, EU IT-systems and fundamental rights*. doi:<https://fra.europa.eu/en/publication/2018/under-watchful-eyes-biometrics-eu-it-systems-and-fundamental-rights>
- Generation 2.0 Joint Announcement. (2020, September 29). *Joint Announcement on the European Pact on Migration and Asylum*. Ανάκτηση από Generation 2.0 for Rights, Equality & Diversity : <https://g2red.org/joint-announcement-on-the-european-pact-on-migration-and-asylum/>
- International Human Rights Program and the Citizen Lab . (2018). *Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada’s Immigration and Refugee System*. Toronto: Faculty of Law, University of Toronto and Munk School of Global Affairs and Public Policy, University of Toronto.
- Joint Statement ECRE. (2020, October 6). *The Pact on Migration and Asylum: to provide a fresh start and avoid past mistakes, risky elements need to be addressed and positive aspects need to be expanded*. Ανάκτηση από European Council on Refugees and Exiles: <https://www.ecre.org/the-pact-on-migration-and-asylum-to-provide-a-fresh-start-and-avoid-past-mistakes-risky-elements-need-to-be-addressed-and-positive-aspects-need-to-be-expanded/>
- Joint statement at Human Rights Council. (2020). *Freedom of association for migrants*. 44th Session of the UN Human Rights Council, Interactive Dialogue with the Special Rapporteur on the Human Rights of Migrants.
- Jones, Ch. (2019). *Data Protection, Immigration Enforcement and Fundamental Rights: What the EU’s Regulations on Interoperability Mean for People with Irregular Status*. Center for European Policy Studies (CEPS) and European Migration Law, Statewatch. PICUM.
- Jones Ch. (2020). *Data Protection and Digital Technologies/ What the EU’s Regulations on Interoperability Mean for People with Irregular Status*. Centre for European Policy Studies (CEPS) and European Migration Law., Statewatch . Platform for International Cooperation on Undocumented Migrant. Ανάκτηση από <https://picum.org/data-protection-and-digital-technologies/>

- Latonero, Hiatt, Napolitano, Clericetti. (2019). *Digital Identity in the Migration & Refugee Context: ITALY CASE STUDY*. Penagos.
- Lum K., Isaac W. (2016, October 7). To predict and serve? (2016) 13(5) Significance 14., p. 1516. *Journal of the Royal Statistical Society*. Ανάκτηση από Journal of the Royal Statistical Society: <https://rss.onlinelibrary.wiley.com/doi/full/10.1111/j.1740-9713.2016.00960.x>
- M. Douo, L. Izuzquiza, M. Silva. (2021). *Lobbying Fortress Europe The making of a border-industrial complex*. Corporate Europe Observatory (CEO). Ανάκτηση από <https://corporateeurope.org/en/lobbying-fortress-europe>
- Molnar, P. (2019). *Emerging Voices: Immigration, Iris-Scanning and iBorderCTRL—The Human Rights Impacts of Technological Experiments in Migration*. Ανάκτηση από <http://opiniojuris.org/2019/08/19/emerging-voices-immigration-iris-scanning-and-iborderctrl-the-human-rights-impacts-of-technological-experiments-in-migration/>
- Molnar, P. (2019, June). New technologies in migration: human rights impacts. *the ETHICS issue*, pp. 7-9.
- Mijatović, D. (2018). *Safeguarding human rights in the era of artificial intelligence*. Commissioner for Human Rights, HUMAN RIGHTS COMMENT, Council of Europe, Strasbourg.
- Network for the Rights of Moving Children. (2018). *Deprivation and restriction of the freedom of unaccompanied children and critical issues for their protection*. Text findings, .
- NIST. (2019, December 19). *Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*. Ανάκτηση από National Institute of Standards and Technology: <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software>
- PICUM. (2020). *Data protection and the “firewall”: advancing the right to health for people in an irregular situation platform for international cooperation on undocumented migrants*. Ανάκτηση από https://picum.org/wp-content/uploads/2020/07/PICUM-Briefing_Data-protection-and-the-firewall_health.pdf
- PICUM. (2020). *How do the new EU regulations on interoperability lead to discriminatory policing?*

PICUM. (2020, October 14). *More detention, fewer safeguards: How the new EU Pact on Migration and Asylum creates new loopholes to ignore human rights obligations*. Ανάκτηση από Platform for International Cooperation on Undocumented Migrants: <https://picum.org/wp-content/uploads/2020/10/More-detention-fewer-safeguards-How-the-new-EU-Pact-on-Migration-and-Asylum-creates-new-loopholes-to-ignore-human-rights-obligations.pdf>

PICUM. (June 2020). Input To EU Consultation On Artificial Intelligence. *Shaping Europe's digital future*. European Commission.

Program for the Rehabilitation of Survivors of Torture . (2017). *"Prometheus"*. Greek Council for Refugees (GCR), Babel Day Centre/Syn-eirmos in co-operation with the Medecins Sans Frontieres . Ανάκτηση από <https://www.projectprometheus.gr/el/%ce%bc%ce%b1%cf%81%cf%84%cf%85%cf%81%ce%af%ce%b5%cf%82-%ce%b5%cf%80%ce%b9%ce%b2%ce%b9%cf%89%cf%83%ce%ac%ce%bd%cf%84%cf%89%ce%bd-%ce%b2%ce%b1%cf%83%ce%b1%ce%bd%ce%b9%cf%83%cf%84%ce%b7%cf%81%ce%af%cf%89/>

Red Cross EU . (2020, December 18). *Minimising the humanitarian impact of immigration detention: time to promote alternatives*. Ανάκτηση από Red Cross EU : <https://redcross.eu/latest-news/minimising-the-humanitarian-impact-of-immigration-detention-time-to-promote-alternatives>

Report from the Commission. (2019). *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*. Final Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Building Trust In Human-Centric Artificial Intelligence . Ανάκτηση από https://openresearch.amsterdam/image/2021/6/8/celex_52020dc0064_en_txt.pdf

Rights, E. U. (2018). *Age assessment and fingerprinting of children in asylum procedures Minimum age requirements concerning children's rights in the EU*. Ανάκτηση από <https://fra.europa.eu/en/publication/2018/age-assessment-and-fingerprinting-children-asylum-procedures-minimum-age>

- Sarantou E, Theododopoulou A. (2019). *Exclusion and exploitation of unaccompanied minors in Greece, Italy and Spain*. Comparative study , Greece Branch of the Rosa Luxemburg Foundation and the Steps Civil Non-Profit Company, HIAS Greece and the Hellenic Refugee Council. Municipality of Athens.
- Satzewich, V. (2014, 21 January 21). Canadian Visa Officers and the Social Construction of “Real” Spousal Relationships. *Canadian Review of Sociology*. Ανάκτηση από <https://onlinelibrary.wiley.com/doi/abs/10.1111/cars.12031>
- Staton B. (2016, May 18). Eye spy: biometric aid system trials in Jordan- But refugees find it restrictive and aid agencies have security concerns. *The New Humanitarian*.
- Statewatch. (2020, November 18). *Frontex: multi-million euro contracts signed while lobby register still in the works* *Frontex Secrecy and transparency EU*. Ανάκτηση από Statewatch : <https://www.statewatch.org/news/2020/november/frontex-multi-million-euro-contracts-signed-while-lobby-register-still-in-the-works/>
- Tsourdi, L. (2020, November 16). *Immigration and asylum law and policy*. Ανάκτηση από Maastricht University: <https://www.maastrichtuniversity.nl/blog/2020/11/immigration-and-asylum-law-and-policy>
- UN Committee on Economic, Social and Cultural Rights (CESCR). (2017, , August 10). *General comment No. 24 (2017) on State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities*. Ανάκτηση από E/C.12/GC/24: <https://www.refworld.org/docid/5beaecba4.html>
- Voule, Clément Nyaletsossi. 2019. “Rights to Freedom of Peaceful Assembly and of Association: Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association.” A/HRC/41/41. United Nations General Assembly Human Rights Council.
- Williams P. , Kind E. (2019). *Data-Driven Policing: The Hardwiring Of Discriminatory Policing Practices Across Europe*. Open Society Foundations. Brussels: European Network Against Racism (ENAR).

Legal Texts

Proposal for a Regulation of the European Parliament and of the Council on Establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) 474 final} Brussels, 12.12.2017 COM (2017) 794 final 2017/0352 (COD)

Accompanying Regulation (EC) No 767/2008 and Regulation (EU), No 1077/2011 and Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) {SWD (2016)}, Brussels, 6.4.2016

Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocol No. 11 Rome, 4.XI.1950

Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5, available at: <https://www.refworld.org/docid/3ae6b3b04.html> [accessed 21 February 2021]

[Directorate-General for Migration and Home Affairs](#) and [European Commission](#). Feasibility study of a Common Identity Repository (CIR) 2018-02-07.

EU Charter of Fundamental Rights Respect of privacy and family life OJ C 202, 7.6.2016, p. 395–395

European Commission- Migration Affairs- Visa Information System (VIS) Brussels, 17.12.2020C(2020) 8000 final 17.12.2020

European Commission New Pact on Migration and Asylum COM (2020) 609 final, 23 September 2020, 21–22.

European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02, available at: <https://www.refworld.org/docid/3ae6b3b70.html> [accessed 21 February 2021]

European Parliament and Council of European Union (2016) Regulation (EU) 2016/679. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>. [accessed 18 July 2021]

Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 OJ L 135, 22.5.2019, p. 85–135

The United Nations General Assembly. 1966. “International Covenant on Civil and Political Rights.” Treaty Series 999 (December): 171.

The United Nations General Assembly. 1966. “International Covenant on Economic, Social, and Cultural Rights.” Treaty Series 999 (December): 171.

UN Committee on the Protection of the Rights of All Migrant Workers and Members of Their Families (CMW), Joint general comment No. 4 (2017) of the Committee on the Protection of the Rights of All Migrant Workers and Members of Their Families and No. 23 (2017) of the Committee on the Rights of the Child on State obligations regarding the human rights of children in the context of international migration in countries of origin, transit, destination and return, 16 November 2017, CMW/C/GC/4-CRC/C/GC/23, available at:

<https://www.refworld.org/docid/5a12942a2b.html> [accessed 14 November 2021]

UN General Assembly, Convention on the Rights of the Child, 20 November 1989, United Nations, Treaty Series, vol. 1577, p. 3, available at:

<https://www.refworld.org/docid/3ae6b38f0.html> [accessed 14 November 2021]

UN General Assembly, Convention Relating to the Status of Refugees, 28 July 1951, United Nations, Treaty Series, vol. 189, p. 137, available at:

<https://www.refworld.org/docid/3be01b964.html> [accessed 14 November 2021]

UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III), available at: <https://www.refworld.org/docid/3ae6b3712c.html> [accessed 18 July 2021]

Jurisprudence

Case of *Abdullahi Elmi And Aweys Abubakar V. Malta*, Council of Europe: European Court of Human Rights (ECtHR) (*Applications nos. [25794/13](#) and [28151/13](#)*) 22 November 2016 FINAL 22/02/2017

Case Of *S. and Marper v. United Kingdom*, Applications nos. 30562/04 and 30566/04, Council of Europe: European Court of Human Rights, 4 December 2008, available at: <https://www.refworld.org/cases,ECHR,4ee21cbe2.html> [accessed 21 February 2021]

Case of *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*-Requests for a preliminary ruling from the High Court (Ireland) and the Verfassungsgerichtshof, Court of Justice of the European Union (Grand Chamber) 8 April 2014 *Digital Rights Ireland Ltd (C-293/12)*

Case of *Maximillian Schrems v Data Protection Commissioner.*, Court of Justice of the European Union (Grand Chamber) of 6 October 2015. C-362/14. ECLI identifier: ECLI:EU:C: 2015:650

Case of *UNv Staatsanwaltschaft Oenburg* (2017) C 9/16 ECLI:EU:C: 2017:483, Case C 278/12 PPU *Atiqullah Adil* (2012) ECLI:EU:C:2012:508, Joined cases C-188/10 and C-189/10 *Aziz Melki* (C-188/10) C-188/10) and *Sélim Abdeli* (C-189/10) (2010) ECLI:EU:C:2010:363. Judgment of the Court of Justice of the European Union (Fifth Chamber) of 14 May 2020.