

# AI-driven migration management procedures: fundamental rights issues and regulatory answers

Mirko Forti\*

AI-DRIVEN MIGRATION MANAGEMENT PROCEDURES: FUNDAMENTAL RIGHTS ISSUES AND REGULATORY ANSWERS

**ABSTRACT:** Artificial Intelligence can represent a valuable resource in managing migration flows. AI algorithms can perform several tasks including border controls, identity checks and predictive policing procedures. However, the utilization of such tools in the migration context raises several issues which must be analyzed and discussed in their implications. The presence of bias in datasets can lead to outcomes detrimental to the already vulnerable conditions of migrants. Furthermore, the inherent opaqueness of AI algorithms working routine does not allow the formulation of a clear accountability framework. This article aims to address these concerns to formulate valid answers from a legal and technological perspective, mainly focusing on the European Union approach to these issues.

**KEYWORDS:** Artificial Intelligence; algorithms; migration; borders; fundamental rights

**SUMMARY:** 1. Introduction – 2. Defining Artificial Intelligence – 3. AI tools in the management of migratory phenomena – 4. AI and migration: the European Union approach – 4.1. iBorderCtrl: AI detection system at the European borders – 4.2. Eurosur system of surveillance – 5. Critical issues and legal challenges in using AI tools to manage migration flows – 5.1. Explicability and black box barrier – 5.2. AI and accountability in the public sector – 6. Fundamental rights issues in managing migration flows with AI tools – 6.1. AI tools and discrimination practices at the borders – 6.2. Data protection principles in the AI-driven migration management procedures – 6.3. AI-driven border controls and the application of the *non-refoulement* principle – 7. Procedural safeguards in AI-driven individual expulsion proceedings – 8. Concluding remarks and recommendations

## 1. Introduction

**A**rtificial Intelligence (AI) algorithms are playing an important role in many sectors of contemporary life. Driverless cars, predictive medicine tools, and automated assistants (chatbot) are just a few examples of the groundbreaking innovations brought by Artificial Intelligence. AI algorithms can represent a factor also in managing migratory flows. Climate change, famine or wars are just some of the reasons behind these migratory phenomena. AI tools can help in speeding up border controls and migrant reception procedures while respecting the fundamental rights of the

---

\* Research Fellow, Sant'Anna School of Advanced Studies. Mail: [mirko.forti@santannapisa.it](mailto:mirko.forti@santannapisa.it). The article was subject to a double-blind peer review process.



people involved and safeguarding internal public order and security. States are therefore considering new instruments, including technological ones, to manage migratory flows in this perspective.<sup>1</sup>

Facial recognition systems, biometric scanners, data collection and storage mechanisms, and predictive processing algorithms are just some of the ways in which digital technologies, and especially Artificial Intelligence tools, are used in immigration management practices.

However, the use of AI instruments in the context of migration raises concerns that need to be analyzed and discussed in their implications. A not carefully regulated use of such tools may exacerbate the vulnerable conditions in which migrants already find themselves.<sup>2</sup> The working routine of AI algorithms is inherently opaque and lacks in terms of transparency. Thus, it may be not possible to control the reasoning process behind the production of a specific outcome. An external human observer could not individuate biases in the processed datasets. The fate of migrants and their families could, therefore, be affected by erroneous and potentially harmful assumptions.<sup>3</sup> Data breaches or system failures should be taken into account in designing migration management procedures involving technological tools. Similar occurrences can have a tremendous impact on the life of migrants.

This paper aims to illustrate the current regulation for the use of technological tools in the migration context. The goal is to understand if the use of Artificial Intelligence algorithms can take place while respecting the rights of migrants.

The first part of the paper focuses on the technical characteristics of Artificial Intelligence algorithms to highlight what impact they can have in the management of migration flows. The second part considers the approach of the European Union to the matter to highlight its possible criticalities. It then proposes a few policy recommendations for ethical and respectful use of Artificial Intelligence tools in the context of migration.

## 2. Defining artificial intelligence

Scholars, philosophers and legislators have provided different definitions of Artificial Intelligence over the years, depending on the perspective considered. The first attempt in this sense included in the definition of Artificial Intelligence those machines capable of using forms of language and performing reasoning processes typical of the human mind.<sup>4</sup> The so-called symbolic artificial intelligence operated on this premise: a representation of machines' logical and decision-making processes understandable for the human mind.<sup>5</sup> Machine learning systems currently in use operate on different assumptions.<sup>6</sup>

<sup>1</sup> P. MOLNAR, *AI and migration management* in M.D. DUBBER, F. PASQUALE, S. DAS (eds), *The Oxford Handbook of Ethics and AI*, Oxford, 2020.

<sup>2</sup> P. MOLNAR, L. GILL, *Bots at the Gate. A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System*, 2018, <https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf> (last visited 11/01/2021).

<sup>3</sup> R. AKHMETHOVA, *How AI is being used in Canada's Immigration Decision Making*, 2020, <https://www.com-pas.ox.ac.uk/2020/how-ai-is-being-used-in-canadas-immigration-decision-making/> (last access 11/01/2021).

<sup>4</sup> J. MCCARTHY et al., *A proposal for the Dartmouth Summer research project on Artificial Intelligence*, 1955, <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf> (last visited 10/03/2021).

<sup>5</sup> J. HAUGELAND, *Artificial Intelligence: the very idea*, Cambridge, 1985.

<sup>6</sup> K. KERSTING, *Machine learning and Artificial Intelligence: two fellow travelers on the quest for intelligent behavior in machines*, in *Frontiers in Big Data*, 1, 6, 2018, 1.



These algorithms can learn new cognitive mechanisms based on experience gained from observing their surroundings through sensors.<sup>7</sup> Machine learning algorithms can elaborate data to find common patterns between information and to forecast future happenings.<sup>8</sup> Deep learning algorithms, an evolution of machine learning systems, process data through neural networks.<sup>9</sup> These data layers are called in this way because of their resemblance with the human brain cells. This is a kind of “diffuse memory” instead of a single central data repository. However, there are drawbacks to using machine learning systems. These technologies require a continuous influx of data, great computational capacity, rely on sensors, and are often ineffective in understanding and reproducing human way of acting.<sup>10</sup> The term Artificial Intelligence, therefore, indicates a set of technologies with multiple characteristics and different areas of application. Thus, it is not easy to provide a single and all-embracing definition of Artificial Intelligence for lawmakers and regulators.

The European Commission provided a definition of AI as a technological system with some degree of autonomy capable of displaying intelligent behaviour and taking decisions according to the environment.<sup>11</sup> More specifically, Artificial Intelligence indicates systems capable of analyzing the surrounding environment before taking actions to reach specific goals. These AI technologies can be entirely software-based, such as voice assistants, search engines or facial recognition systems, or embedded in hardware devices like autonomous vehicles or advanced drones and robots.<sup>12</sup> The independent high-level expert group set up by the European Commission provided a new definition of Artificial Intelligence.<sup>13</sup> These are systems acting in the virtual or physical dimension to accomplish a given goal. They collect data by perceiving the surrounding environment and decide the best reasoning pattern to take to reach the final scope. AI systems can use symbolic rules either a numerical model to perform and adapt their working routine to the circumstances affected by their previous actions.

Defining artificial intelligence is a fundamental step to understand how AI tools work and what impact they can have in managing migration flows.

---

<sup>7</sup> P. FLACH, *Machine Learning: the Art and Science of Algorithms that make sense of data*, Cambridge, 2012, 13.

<sup>8</sup> J. BURREL, *How the Machine “Thinks”: Understanding Opacity in Machine Learning Algorithms*, in *Big Data & Society*, 3, 2016, 1.

<sup>9</sup> R. DIAS, A. TORKAMANI, *Artificial Intelligence in Clinical and Genomic Diagnostics*, in *Genome Medicine*, 11, 70, 2019, 1.

<sup>10</sup> Editorial, *Materializing Artificial Intelligence*, in *Nature Machine Intelligence*, 2, 2020, 653.

<sup>11</sup> Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, COM (2018) 795 final, 07/12/2018, *Coordinated Plan on Artificial Intelligence*.

<sup>12</sup> Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, COM (2018) 237 final, 25/04/2018, *Artificial Intelligence for Europe*.

<sup>13</sup> Independent High-Level Expert Group on Artificial Intelligence, *A definition of AI: main capabilities and disciplines*, <https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines> (last visited 10/03/2021).



### 3. Ai tools in the management of migratory phenomena

Canada is developing a system of predictive analytics to support national authorities in assessing immigrants' applications.<sup>14</sup> The aim is to individuate any potential sign of fraud or illicit application for an entry permit. Furthermore, AI algorithms can evaluate if applicants could represent a risk for national safety.<sup>15</sup> More specifically, Canadian immigration officers could use AI instruments to make immigrants going under screening for admissibility proceedings according to section 33 of the Immigration and Refugee Protection Act (IRPA)<sup>16</sup> to determine if an alien subject could enter the Canadian borders. Algorithms are trained to evaluate the completeness of an application and if it is legally compliant or fraudulent.

However, the Canadian government's use of artificial intelligence systems to control national borders raises some concerns that deserve analysis.<sup>17</sup> The definition of concepts such as "fraud" or "risk" is not unambiguous. Preferring one interpretation of these terms over another can affect the work of the algorithms. There is a lack of clarity as to which entities are entitled to access information regarding migrants and refugees seeking to enter Canadian territory. It is likewise unclear whether public offices that have such data available can share them with other entities. Artificial intelligence systems are failure-prone machines. People who see their data collected and processed by such algorithms should be informed about the margin of error that the Canadian government considers acceptable in such data-driven border control procedures. Migrants and refugees should also be informed about the role played by AI algorithms in procedures involving them. More specifically, they should be aware of their right to ask for redress in case of algorithmic misconduct.

When migration management operations are related to national security matters, border controls and identity checks procedures could become more opaque and less transparent. Despite recent rulings of the Canadian Supreme Court against this possibility,<sup>18</sup> immigration officers can withhold information collected during security proceedings, for instance, in case of suspect terrorism activities, according to section 83 (1) and 85.4 (1) of the IRPA. The use of these datasets in the context of AI migration management could eventually lead to digital surveillance concerns, in spite of the privacy rights of people involved.

As far as national security issues are concerned, the United States government is using AI-driven technologies, such as drones and cameras, to patrol borders and to fight against illegal migration and

<sup>14</sup> P. MOLNAR, L. GILL, *op.cit.*

<sup>15</sup> N. KEUNG, *Canadian Immigration applications could soon be assessed by computers*, in *The Star*, 2017, <https://www.thestar.com/news/immigration/2017/01/05/immigration-applications-could-soon-be-assessed-by-computers.html>, (last visited 12/01/2021).

<sup>16</sup> Immigration and Refugee Protection Act (IRPA) (S.C. 2001, c.27).

<sup>17</sup> P. MOLNAR, L. GRILL, *op. cit.*

<sup>18</sup> *Charkaoui v. Canada (Minister of Citizenship and Immigration)*, [2007] SCC 9; *Canada (Minister of Citizenship and Immigration) v. Harkat*, [2014] SCC 37.



human trafficking.<sup>19</sup> The United States unveiled the Extreme Vetting project<sup>20</sup> in 2017 on the legal ground of the executive order issued by the Trump Presidency with the aim to protect the national territory from foreign terrorists.<sup>21</sup> According to this project, automated decision-making systems would assess the application for entering the United States. More specifically, AI tools would determine if the foreign applicant may be a positive addition to the community or otherwise a possible threat for national security. Algorithms would process data collected from government agencies archives and public sources online like social media account to perform these tasks. However, such databases may contain biased information and the assessing process could not be reliable at all.<sup>22</sup> For instance, alien claimants and applicants could modify their behavior if they are aware of being under investigation.<sup>23</sup> Successively, the United States conceded that a similar assessment program could seriously affect the human rights of people involved in several ways, including their privacy and right to identity. Thus, the national immigration agency abandoned the idea of a complete automatization of the vetting process.<sup>24</sup>

The Italian government is considering using facial recognition algorithms in migration management.<sup>25</sup> The SARI (*Sistema Automatico Riconoscimento Immagini*) system would make it possible to verify the authenticity of photos used in identification documents. The border guards would have to compare these photos with the information present in the AFIS (*Automated Fingerprint Identification System*) database managed by the Italian Police. The Italian Data Protection Authority considered that this procedure did not infringe the privacy rights of the persons involved.<sup>26</sup> On the other hand, the intention to use the same systems to monitor the various phases of migrant disembarkation and film any illegal activities to identify those involved raises some concerns from the data protection perspective. At present, the SARI system is not operational for these purposes.

<sup>19</sup> O. SOLON, *Surveillance Society: has technology at the US-Mexico border gone too far?*, in *The Guardian* June 2018, <https://www.theguardian.com/technology/2018/jun/13/mexico-us-border-wall-surveillance-artificial-intelligence-technology>, (last visited 12/01/2021).

<sup>20</sup> A. GLASER, *ICE Wants to Use Predictive Policing Technology for its "Extreme Vetting" Program*, in *Slate*, 2017, <https://slate.com/technology/2017/08/ice-wants-to-use-predictive-policing-tech-for-extreme-vetting.html>, (last visited 12/01/2021).

<sup>21</sup> Presidency of the United States, Executive Order 13769, 27 January 2017, 82 FR 8977, *Executive Order Protecting the Nation from Foreign Terrorist Entry into the United States*, [2017], <https://www.whitehouse.gov/presidential-actions/executive-order-protecting-nation-foreign-terrorist-entry-united-states/>, (last visited 12/01/2021).

<sup>22</sup> P. MOLNAR, L. MCGILL, *op. cit.*

<sup>23</sup> B. ROOT, *US Immigration Officials Pull Plug On High-Tech Extreme Vetting*, in *Human Rights Watch*, 2018, <https://www.hrw.org/news/2018/05/18/us-immigration-officials-pull-plug-high-tech-extreme-vetting>, (last visited 12/01/2021).

<sup>24</sup> N. DUARTE, *ICE Finds Out It Can't Automate Immigration Vetting. Now What*, in *Center for Democracy and Technology*, 2018, <https://cdt.org/insights/ice-cant-automate-immigration-vetting/>, (last visited 12/01/2021).

<sup>25</sup> R. COLUCCINI, *Lo scontro Viminale-Garante della Privacy sul riconoscimento facciale in tempo reale*, in *IRPI*, 2021, <https://irpimedia.irpi.eu/viminale-garante-privacy-riconoscimento-facciale-in-tempo-reale/>, (last visited 18/03/2021).

<sup>26</sup> Garante per la Protezione dei Dati Personali, *Sistema Automatico di ricerca all'identità di un volto*, 26/07/2018, doc.n.9040256, <https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9040256>, (last visited 18/03/2021).



AI algorithms can help states in the reception and integration operations of migrants and refugees who have arrived within the national territory. Switzerland is currently using algorithmic systems to figure out how best to relocate such individuals within its cantons. Variables such as the population of the various areas and their cultural diversity are taken into account.<sup>27</sup> The United States government and resettlement agencies are considering to use similar algorithms to find the most suitable spot for refugees to relocate according to their cultural background and job skills.<sup>28</sup>

AI tools could also represent a valuable instrument to overcome cultural divergencies and language misunderstandings.<sup>29</sup> Germany is running pilot projects exploiting AI technologies to perform tasks as dialect recognition, name transliteration and real-time translation. This solution could help in reducing the time spent in assessing immigration application which would otherwise require the intervention of experts like linguists and translators. Machine-learning algorithms process data to provide predictions about future outcomes, even in the migratory context.<sup>30</sup> Thus, States like Sweden are deploying such algorithms to forecast future migration flows in order to be prepared for the next humanitarian crisis.<sup>31</sup>

The European Union is carefully considering the use of artificial intelligence algorithms in migration management operations. However, the deployment of these tools must be done with respect for the fundamental rights of the people involved, primarily migrants and refugees.

#### 4. Ai and migration: the european union approach

The recently released New Pact on Migration and Asylum explains the new European Union approach to migration issues.<sup>32</sup> It consists of several normative and regulatory proposals to reform the entire migration management system. The reform of European border control and monitoring procedures also includes the use of advanced technological tools in the migration context. The European Union is developing an AI approach to the issues related to migration management.<sup>33</sup> Lawmakers and migration

<sup>27</sup> K. BANSAK et al., *Improving refugee integration through data-drive algorithmic assignment*, in *Science*, 359(6373), 2018, 325.

<sup>28</sup> A. SHASHKEVICH, *Stanford Scholars Develop New Algorithm to Help Resettle Refugees and Improve their Integration*, in *Stanford News*, 2018, <https://news.stanford.edu/2018/01/18/algorithm-improves-integration-refugees/> (last visited 17/03/2021).

<sup>29</sup> J. TANGERMANN, *Documenting and Establishing Identity in the Migration Process. Challenges and Practices in the German Context*, German Federal Office for Migration and Refugees Working Paper, 76, 2017, [https://ec.europa.eu/homeaffairs/sites/homeaffairs/files/11a\\_germany\\_identity\\_study\\_final\\_en.pdf](https://ec.europa.eu/homeaffairs/sites/homeaffairs/files/11a_germany_identity_study_final_en.pdf), (last visited 12/01/2021).

<sup>30</sup> A. BEDUSCHI, *International Migration Management in the Age of Artificial Intelligence*, in *Migration Studies*, 2020, 1.

<sup>31</sup> M. CARAMMIA, J.C. DUMONT, *Can We Anticipate Future Migration Flows?*, in *OECD Migration Policy Debates*, 2018, <https://www.oecd.org/els/mig/migration-policy-debate-16.pdf>, (last visited 12/01/2021).

<sup>32</sup> Press Release, *A fresh start on migration: building confidence and striking a new balance between responsibility and solidarity*, 2020, [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_20\\_1706](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1706), (last visited 18/03/2021).

<sup>33</sup> Commission Report, *Opportunities and Challenges for the Use of Artificial Intelligence in Border Control, Migration and Security*, <https://op.europa.eu/en/publication-detail/-/publication/c8823cd1-a152-11ea-9d2d-01aa75ed71a1/language-en>, (last visited 12/01/2021).

practitioners identified different areas where AI algorithms could play a fundamental role in this context, from risk assessment procedures to detecting illegal cross border activities.

Frontex, the European border control agency, is carefully considering new ways to secure European borders and to improve its technological capabilities.<sup>34</sup> It is following the development of several projects financed with research funds from the Horizon 2020 programme. Frontex recently signed an agreement with the Directorate-General for Migration and Home Affairs of the European Commission (DG-HOME) for the supervision and implementation of research projects related to border security issues.<sup>35</sup>

The TRESPASS project aims to implement a risk-based approach in the operations of controlling national borders and regulating the entry of foreigners into the national territory. Algorithms collect and process data to identify, according to certain indicators, the level of “risk” of each possible entry within the state borders.<sup>36</sup> The ROBORDER project aims to implement a fully automated and unmanned border surveillance system. More specifically, it is a complex of mobile robotic vehicles capable of operating on any surface.<sup>37</sup> The FOLDOUT project aims to create a platform for real-time surveillance of state borders. A set of sensors collects information to inform border guards about possible threats along the borders.<sup>38</sup> The aim is to immediately detect any illegal cross-border movement. These are just a few examples of projects that have been considered. Frontex has also evaluated other solutions over the years: digital platforms for remote identification of vessels, biometric scanning and heartbeat recognition systems (to detect migrants hiding in vehicles and containers attempting to cross European borders illegally).<sup>39</sup>

Algorithmic system can also work for lie detection purposes. The idea is to use these tools to detect if people requesting visas or entry permit are lying about their credentials through the processing of biometric data like facial expressions.

#### 4.1. iBorderCtrl: AI detection system at the european borders

The iBorderCtrl project consists of a complex algorithmic system to detect false or contradictory statements made by migrants to border control. A digital avatar of a policeman asks travellers questions about their route, where they are coming from and their intentions, while a camera records the reactions of individuals. A QR code is then issued at the end of the questions for individuals to present at

---

<sup>34</sup> Press Release, *Frontex helping to bring innovation to future border control*, 2020, <https://bit.ly/3uKu19B> (last visited 18/03/2021).

<sup>35</sup> Terms of Reference between Directorate-General for Migration and Home Affairs of the European Commission and the European Border and Coast Security Agency, [https://ec.europa.eu/home-affairs/sites/homeaffairs/files/20200206\\_tor-ec-dg-home-frontex.pdf](https://ec.europa.eu/home-affairs/sites/homeaffairs/files/20200206_tor-ec-dg-home-frontex.pdf), (last visited 19/03/2021).

<sup>36</sup> A complete analysis of the TRESPASS project is available here <https://www.tresspass.eu/The-project> (last visited 19/03/2021).

<sup>37</sup> The website of the ROBORDER project is available here <https://roborder.eu/the-project/project-structure/> (last visited 19/03/2021).

<sup>38</sup> More information about the FOLDOUT project are available here <https://foldout.eu/> (last visited 19/03/2021).

<sup>39</sup> F. CHIUSI, *Poliziotti virtuali, riconoscimento facciale, tecnologie biometriche, scoring algoritmico per gestire il controllo dei confini: è questa l'Europa dei diritti?*, in *Valigia Blu*, 2021, <https://www.valigiablu.it/sorveglianza-tecnologia-confini-europa/> (last visited 19/03/2021).





border controls. The border guards can scan the code to check the veracity of the answers. If the questioning is unsuccessful, travellers may be subject to further checks.

The iBorderCtrl working routine has given rise to a number of concerns about its effectiveness and fairness.<sup>40</sup> Researchers tested the system to find out a 75% level of accuracy.<sup>41</sup> However, it should be noted that the study group was not adequately proportioned in terms of factors such as gender or ethnicity. Member of the European Parliament Patrick Breyer filed a lawsuit against the European Commission seeking an explanation of its decision to fund the iBorderCtrl system.<sup>42</sup> The politician asserted that there is no scientific evidence on the validity of these lie detection mechanisms.<sup>43</sup> He also complained about a lack of transparency regarding the actual operation of the lie detector system and expressed concerns that this technology could also be used for commercial purposes by private parties. Further investigations have shown that the algorithmic technology of the iBorderCtrl system takes into account variables such as people's ethnic origin, thus leaving room for suspicion of discriminatory results.<sup>44</sup> Algorithms should consider cultural divergencies and different societal backgrounds to interpret facial expressions and social behaviours correctly. AI tools require a large amount of data to perform similar tasks and how they process these inputs could produce biased outcomes. Avoiding collecting information about a specific segment of the population or otherwise designing the algorithms to recognize particular "lying signals" instead of others could seriously influence the production of outcomes. Furthermore, it is not clear if AI-driven lie detectors could assess in the proper way signs of trauma: a migrant shocked by a perilous journey shall react to questions peculiarly.<sup>45</sup>

#### 4.2. Eurosur system of surveillance

The European Border Surveillance System (Eurosur) takes place at the European border.<sup>46</sup> The Member States and Frontex jointly operate this system to increase situational awareness of what is happening at the European borders and increase the reaction capabilities of border guards. Eurosur aims to combat cross-border criminal phenomena, such as trafficking in human beings, and to safeguard the safety of migrants. Eurosur consists of a network of surveillance and information exchange systems. Each Member State coordinates a national hub to collect information on what is happening at its border. Meanwhile, Frontex is supervising the entire European framework.

<sup>40</sup> R. GALLAGHER, L. JONA, *We tested Europe's new lie detector for travelers – and immediately triggered a false positive*, in *The Intercept*, 2019, <https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector/> (last visited 19/03/2021).

<sup>41</sup> K. CROCKETT et al., *Intelligent deception detection through Machine Based interviewing*, Conference Paper, 2018, 1.

<sup>42</sup> Action brought on 15 March 2019, *Breyer v. Commission*, Case T-158/19.

<sup>43</sup> N. LOMAS, 'Orwellian' AI lie detector project challenged in EU court, in *Tech Crunch*, 2021, <https://techcrunch.com/2021/02/05/orwellian-ai-lie-detector-project-challenged-in-eu-court/>, (last visited 19/03/2021).

<sup>44</sup> U. BACCHI, *High-tech lie detector used at Europe borders face scrutiny*, 2021, <https://www.reuters.com/article/europe-tech-court-idUSL8N2KB346>, (last visited 19/03/2021).

<sup>45</sup> H. EVANS CAMERON, *Refugee Law's Fact-Finding Crisis: Truth, Risk and the Wrong Mistake*, Cambridge, 2018, 76.

<sup>46</sup> Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur), OJ L 295, 06/11/2013, 11.





The aim is to have a constantly updated picture of the situation at the European borders. Frontex supervises the deployment of surveillance tools to detect cross border movements and thus to facilitate the interception of supposedly illegal activities. Border guards can rely on sophisticated technologies like platforms with sensors, satellite images, UAVs. As far as Artificial Intelligence systems are concerned, Frontex is using algorithms to track suspicious vessels' movements and to forecast their possible final destination.

Eurosur is therefore adopting a preventive approach. This system assesses suspicious movement in the nearby European frontiers trying to anticipate the occurrence of border-crossing activities.<sup>47</sup> It represents a less visible way of controlling borders than the traditional approach of deploying guards and police forces on the frontier line.<sup>48</sup> The functioning of Eurosur ensures that state control functions are not limited to the national territory and are anticipated before the possible criminal event takes place.<sup>49</sup> Eurosur, therefore, carries out an assessment of possible vulnerabilities at national borders: in this way, migrants are seen as a potential crisis factor.<sup>50</sup>

## 5. Critical issues and legal challenges in using ai tools in the management of migration flows

The use of artificial intelligence systems in migration management has undoubted benefits. Algorithms allow for a reduction in the time it takes to collect the data needed to make administrative decisions such as issuing visas. They enable more efficient controls of national borders and prevent the occurrence of possible national security threats. Nonetheless, lawmakers and regulators need to consider several elements that can exacerbate the inherent vulnerability faced by migrants and refugees.

### 5.1. Explicability and black box barrier

The reasoning routine of modern AI algorithms is inherently opaque and undetectable. More specifically, they do not provide understandable explanations of their outputs. It is possible to understand the technological mechanisms that led the algorithm to produce a certain result based on certain inputs. Machine learning algorithms process a set of inputs in a machine-readable format: a series of 0s and 1s arranged according to binary code. Scientists can make assumptions about which strings of code the algorithm followed to formulate its output. Nevertheless, a human observer cannot understand the logic behind the resulting outcomes.<sup>51</sup> This inherent lack of transparency is known as black box barrier of Artificial Intelligence.<sup>52</sup> Efforts to explain the logic behind the reasoning patterns of machine

<sup>47</sup> J. JEANDESBOZ, *Beyond the Tartar steppe: EUROSUR and the ethics of European border control practices*, in J.P. BURGESS, S. GUTWIRTH (eds.), *A threat against Europe? Security, Migration and integration*, Bruxelles, 2012, 111.

<sup>48</sup> D. BIGO, *Globalized (in)security: the field and the ban-opticon*, in D. BIGO, A. TSOUKALA (eds.), *Terror, insecurity, liberty. Illiberal practices of liberal regimes: the (In)security games*, New York, 2008, 10.

<sup>49</sup> M. TAZZIOLI, *Spy, track and archive: the temporality of visibility in Eurosur and Jora*, in *Security Dialogue*, 49, 4, 2018, 272.

<sup>50</sup> M. TAZZIOLI, *op.cit.*

<sup>51</sup> D. CASTELVECCHI, *Can We Open the Black Box of AI*, in *Nature*, 2016, <https://www.nature.com/news/can-we-open-the-black-box-of-ai-1.20731> (last visited 12/01/2021).

<sup>52</sup> Y. BATHAEE, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, in *Harvard Journal of Law and Technology*, 31, 2018, 889.



learning algorithms have had little success to date.<sup>53</sup> It is therefore not technologically possible to understand the rationale behind an algorithmic output. Not being able to understand the motivations behind public decisions raises ethical and legal concerns. The understandability of public actions, like judicial acts, is a crucial factor.<sup>54</sup>

However, Artificial Intelligence tools that are less understandable are usually the ones that get more reliable results.<sup>55</sup> A balance between explicability and the performance of the algorithm must be found. Lawmakers and regulators should take into account the scope of application of the given algorithm in this regard. Several scholars have argued for a principle of explicability of Artificial Intelligence.<sup>56</sup> According to this principle, humans must be able to obtain clear, precise and understandable explanations for the decision-making process adopted by the algorithms. Applying the principle of explicability would allow the maintenance of effective human control over the operation of the algorithms.<sup>57</sup> Humans would be morally responsible for the operation of AI systems and how algorithmic products are employed. The ability to understand the logic behind a given algorithmic decision will allow people to accept it, question it, or even overturn it.<sup>58</sup>

Understanding the factors that produced a particular algorithmic result is particularly important in the context of migration management. Human operators need to know whether algorithms base their operations on discriminatory or unnecessary elements. Facial recognition systems could identify specific individuals as national security threats because of their facial features. Algorithms could suggest denying entry visas to a given category of people based on their ethnic background. Artificial intelligence tools used for humanitarian purposes or in the management of refugee camps could exclude certain people from receiving essential services based on factors such spoken language or national origin. These are just a few examples of how the use of algorithmic systems in the migration context can exacerbate the vulnerable conditions in which migrants and refugees find themselves. Prejudicial and discriminatory attitudes can propagate and expand without being curbed due to the undetectability of the reasoning process of the algorithms. The use of predictive models generated by data-driven algorithms can discriminatively influence the decision-making process of human actors.<sup>59</sup> This can also happen in the context of migration if the datasets collected have shortcomings or biases that exclude certain individuals from enjoying specific rights, such as freedom of movement from one state to another

<sup>53</sup> R. GUIDOTTI et al., *A survey of methods for explaining black box models*, in *ACM Computer Surveys*, 51, 5, 2018, 1.

<sup>54</sup> S. ROBBINS, *A misdirected principle with a catch: explicability for AI*, in *Minds and Machines*, 29, 2019, 495.

<sup>55</sup> G. SARTOR, F. LAGIOIA, *The impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence*, [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS\\_STU\(2020\)641530\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf) (last visited 11/03/2021).

<sup>56</sup> L. FLORIDI ET AL., *AI4 people – An ethical framework for a good AI society: opportunities, risks, principles, and recommendations*, in *Minds and Machines*, 28, 2018, 689; L. H. GILPIN ET AL., *Explaining explanations: an overview of interpretability of machine learning*, <https://arxiv.org/abs/1806.00069> (last visited 12/03/2021).

<sup>57</sup> F. SANTONI DE SIO, J. VAN DEN HOVEN, *Meaningful human control over autonomous system: a philosophical account*, in *Frontiers in Robotics and AI*, 2018, <https://www.frontiersin.org/articles/10.3389/frobt.2018.00015/full> (last visited 12/03/2021); S. ROBBINS, *AI and the path to envelopment: knowledge as a first step towards the responsible regulation and use of AI-powered machines*, in *AI & Society*, 35, 2020, 391.

<sup>58</sup> S. ROBBINS, *A misdirected principle with a catch: explicability for AI*, cit.

<sup>59</sup> B. A. WILLIAMS ET AL, *How algorithms discriminate based on data they lack: challenges, solutions, and policy implications*, in *Journal of Information Policy*, 8, 2018, 78.



or receiving humanitarian help. Thus, this study argues the necessity of a clear accountability framework regulating the use of algorithmic products in the public decision-making sphere.

## 5.2. AI and accountability in the public sector

The deployment of AI systems is radically transforming the decision-making process of public actors. The growing importance of Artificial Intelligence in the public sector raises important concerns about oversight mechanisms and accountability framework.<sup>60</sup>

Government offices are using digital technologies because they find them efficient, “neutral” and low cost. However, these innovations are revolutionizing the very nature of these offices. They radically challenge the traditional notion of public bodies transforming prerogatives like the exercise of administrative discretion.<sup>61</sup>

This is especially true in policing and law enforcement activities.<sup>62</sup> Algorithms can find hidden patterns among the analyzed data to predict future occurrences, such as criminal activity or whether individuals will be able to pay their debts. However, the operation of predictive policing algorithms is subject to the risk of failure and potentially disastrous consequences.<sup>63</sup> Processing unreliable data can lead to replicating biases and discriminatory attitudes, even in the migration context. Refusing to grant entry visas to individuals of a particular ethnicity then becomes a shared and recognized practice in the algorithms’ training data. Thus, they will guide subsequent decisions in the same direction.<sup>64</sup>

The relative obscurity and lack of transparency inherent in the cognitive pathway of artificial intelligence algorithms mean that it is often not possible to identify the presence of these biases and the persistence of these loop mechanisms that propagate these discriminatory outputs.<sup>65</sup> The growing importance of artificial intelligence systems in public decision-making and the resulting risk for public offices to make decisions influenced by algorithmic biases requires a careful study of the accountability system.

The concept of accountability requires every actor to explain their activities to a specified audience who can then judge their actions and take the appropriate consequences.<sup>66</sup> Algorithmic accountability in the public sector means understanding how public bodies can use algorithmic outputs in their

---

<sup>60</sup> N. DIAKOPOULOS, *Algorithmic accountability reporting: on the investigation of black boxes*, 2014, <https://academiccommons.columbia.edu/doi/10.7916/D8ZK5TW2> (last visited 15/03/2021); J. B. BULLOCK, *Artificial Intelligence, discretion and bureaucracy*, in *The American Review of Public Administration*, 49, 7, 2019, 751; M. BUISOC, *Accountable Artificial Intelligence: holding algorithms to account*, in *Public Administration Review*, 2020, 1.

<sup>61</sup> J. T. BARTH, E. ARNOLD, *Artificial Intelligence and administrative discretion: implications for Public Administration*, in *The American Review of Public Administration*, 29, 4, 1999, 332.

<sup>62</sup> L. B. MOSES, J. CHAN, *Algorithmic prediction in policing: assumptions, evaluation, and accountability*, in *Policing and Society*, 28, 7, 2018, 806; M. CATANZARITI, *Enhancing policing through algorithmic surveillance*, in L. MARIN, S. MONTALDO (eds), *The Fight Against Impunity in EU Law*, London, 2020, 239.

<sup>63</sup> C. RUDIN, *Stop explaining black box machine learning models for high stake decisions and use interpretable models instead*, in *Nature Machine Intelligence*, 1, 206, 2019, 15.

<sup>64</sup> B. LEPRI et al., *Fair, transparent and accountable algorithmic decision-making process. The premise, the proposed solutions and the challenges*, in *Philosophy and Technology*, 31, 2018, 611; M. BUISOC, *op.cit.*, 2.

<sup>65</sup> M. BUISOC, *op. cit.*, 2

<sup>66</sup> M. BOVENS, *Analysing and assessing accountability: a conceptual framework*, in *European Law Journal*, 13, 4, 2007, 447.

decision-making process. In other words, if human observers are capable of auditing, interrogating and understanding the given AI outcome before taking any relevant decision on its base.<sup>67</sup>

This may not be possible for several reasons. This study has already addressed the issue of algorithm explicability. The so-called black box barrier may prevent an external human observer from understanding the reasoning process of a given algorithm.

Understanding of automated decision mechanisms may be further limited by intellectual property issues.<sup>68</sup> Government offices using privately sourced algorithms must therefore rely on the manufacturers and on their willingness to report any errors in the system and take action accordingly.<sup>69</sup> Thus, AI providers have an important role in public decision-making. Implementing specific values in the algorithm's working routine is a political choice. It can influence the final predictive results and consequently benefit certain individuals over others.<sup>70</sup> Public officials may do not have full control over which values to be pursued through their actions.<sup>71</sup>

Defining what values the algorithms used in migration management should pursue is a particularly important question. Prioritizing the efficiency of border control operations over the reception of migrants and refugees can have devastating consequences on the lives of the people involved. The context of migration involves individuals from diverse cultural backgrounds. AI algorithm providers may have calibrated their systems to a notion of certain principles that are not understandable outside of their national borders. European and international regulations deal with a concept of privacy formed in "Western" culture. According to this approach, privacy is an essential element for the self-fulfillment of the individual as a person.<sup>72</sup> Cultures that do not accept such an individualistic approach might recognize a different notion of privacy.<sup>73</sup> Algorithms must take into account these different perspectives to produce reliable results that can be used by public decision makers in managing migration flows. An efficient accountability framework should provide oversight mechanisms capable of maintaining meaningful human control over the utilization of AI outputs. Assessment procedures should be put in place to test the availability of AI systems according to the different sectors of the Public Administration.<sup>74</sup> Independent third parties should also conduct ongoing testing to assess the reliability of algorithms used in various migration management tasks. More specifically, they should assess the need to calibrate the algorithms according to the circumstances (origin of migration flows, societal and cultural background of people involved etc.) to obtain reliable results and protect the rights of migrants and refugees.

<sup>67</sup> M. BUISOC, *op.cit.*, 4.

<sup>68</sup> N. DIAKOPOULOS, *op.cit.*

<sup>69</sup> M. BUISOC, *op.cit.*, 5.

<sup>70</sup> M. M. YOUNG, J. B. BULLOCK, J. D. LACY, *Artificial discretion as a tool of governance: a framework for understanding the impact of Artificial Intelligence on Public Administration*, in *Perspectives on Public Management and Governance*, 2, 4, 2019, 301.

<sup>71</sup> P. A. BUSCH, H. Z. HENRIKSEN, *Digital discretion: a systematic literature review of ICT and street-level discretion*, in *Information Polity*, 23, 1, 2018, 3.

<sup>72</sup> L. A. BYGRAVE, *Privacy protection in a global context – A comparative overview*, in *Scandinavian Studies in Law*, 47, 2004, 319.

<sup>73</sup> L. A. BYGRAVE, *Privacy and data protection in an International perspective*, in *Scandinavian Studies in Law*, 56, 2010, 176.

<sup>74</sup> M. BUISOC, *op. cit.*, 10.

## 6. Fundamental rights issues in managing migration flows with ai tools

The characteristics of algorithmic functioning outlined above may infringe several fundamental rights as stated in International Treaties. More specifically, proper regulation of AI tools in the migration context should formulate appropriate safeguards to avoid discriminatory attitudes, the infringement of data protection rights and to ensure the application of the principle of *non-refoulement*.

### 6.1. AI tools and discrimination practices at the borders

The principle of non-discrimination is one of the fundamental cores of International Human Rights Law. The Universal Declaration of Human Rights (UDHR)<sup>75</sup> states that all humans are born free and equal in dignity and rights (art.1). Furthermore, no one should be subjected to any form of discrimination based on elements like, for instance, sex, race or religion (art.4). Likewise, every human is to be considered equal before the law (art.7). The European Convention on Human Rights (ECHR)<sup>76</sup> affirms that the enjoyment of the freedoms and rights states by the ECHR shall be secured without any discrimination on the basis of elements like sex, language, religion etc. (art.14). The Charter of Fundamental Rights of the European Union (CFREU)<sup>77</sup> prohibits any form of discrimination (art.21). Art 10 of the TFEU requires the European Union to implement its policies and actions fighting including the fight against any form of exclusion and discrimination.<sup>78</sup>

According to the EU approach, AI systems used for border controls only involve third-country nationals. European citizens enjoy the right of freedom of movement within the territory of the European Union. This situation contributes to reinforcing the false identification of the migrant as a possible threat to public safety.<sup>79</sup> Furthermore, it creates an inequality of treatment between Europeans and immigrants.<sup>80</sup>

As far as the migratory context is concerned, biased datasets and how they can influence algorithmic outcomes are the main issues. Adopting AI-driven procedures for managing migration purposes could exacerbate discriminatory attitudes already embedded in the algorithms.<sup>81</sup> AI algorithms may suggest to border guards that specific individuals must undergo further checks based on discriminatory biases such as ethnicity. The discriminatory attitude of the algorithms tends to be self-perpetuating because it influences their training data. Excluding a certain category of people from the possibility of entering

<sup>75</sup> General Assembly of the United Nations, Resolution 217A (III), 8 December 1948, Universal Declaration of Human Rights, [1948], [https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A\\_RES\\_217\(III\).pdf](https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_217(III).pdf), (last visited 12/01/2021).

<sup>76</sup> Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, [https://www.echr.coe.int/Documents/Convention\\_ENG.pdf](https://www.echr.coe.int/Documents/Convention_ENG.pdf), (last visited 12/01/2021).

<sup>77</sup> Charter of Fundamental Rights of the European Union, 18 December 2000, OJ C364/3.

<sup>78</sup> Consolidated Version of the Treaty on the Functioning of the European Union, OJ C 326, 26/10/2012, 47.

<sup>79</sup> L. NUNZIATA, *Immigration and crime: evidence from victimization data*, in *Journal of Population Economics*, 28, 2015, 697

<sup>80</sup> C. BLASI CASAGRAN, *Fundamental rights implications of interconnecting migration and policing databases in the EU*, in *Human Rights Law Review*, 21, 2021, 433.

<sup>81</sup> N. TURNER LEE ET AL., *Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms*, 2019, <https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/>, (last visited 12/01/2021).

into Europe, or at least hindering their movements, based on algorithmic prejudices will make these individuals commit illegal acts.<sup>82</sup> The commission of actions such as illegal migration or cross-border crimes will reinforce the algorithmic bias. These technological systems are not neutral concerning factors such as nationality or ethnicity, as demonstrated in the iBorderCtrl case. The functioning of these technologies could have an impact on the already vulnerable conditions of individuals belonging to minority groups.<sup>83</sup>

## 6.2 Data protection principles in the ai-driven migration management procedures

The right to privacy is a fundamental element for the freedom and self-dignity of a person.<sup>84</sup> It allows every individual to reach a proper intellectual and emotive autonomy. The concept of privacy is continuously changing and evolving following the mutating need of human society.

The UDHR states the right to privacy (art.12): everyone has the right to preserve his/her private life from intrusions of third parties. The ICCPR underlines the need for adequate safeguards also for the reputational sphere of the individual (art.17). The United Nations recently recognized that digital technologies could have a serious impact on privacy rights. More specifically, they may lead to mass surveillance mechanisms which impinge human freedom.<sup>85</sup> According to the General Assembly, people hold the same rights offline and online.<sup>86</sup> States should act to ensure an adequate level of protection for privacy in digital telecommunication. The right to privacy is also recognized on a regional level. For instance, the ECHR protects the private and family life of every individual, including the inviolability of his/her communications (art.8). Likewise, the CFREU recognizes the right to privacy and data protection for every individual. Furthermore, it proclaims that every data processing activity shall follow the principles of fairness, transparency, lawfulness and according to predetermined goals (art.8).

The use of AI systems in the migration context may have a severe impact on the principles enshrined in the GDPR.<sup>87</sup> Data collection and elaboration procedures shall be carried on accordingly with the values of fairness, transparency and lawfulness (Art.5).

The transparency principle indicates data processing activities shall be conducted openly and clearly about who is elaborating data and how. The black box barrier jeopardizes the application of this principle. As far as the migration context is concerned, different subjects like Frontex or national law

<sup>82</sup> P. WILLIAMS, E. KIND, *Data-driven policing: the hardwiring of discriminatory policing practices across Europe*, 2019, <https://bit.ly/34U3b4p>, (last access 22/03/2021).

<sup>83</sup> *Ibidem*.

<sup>84</sup> A.F. WESTIN, *Privacy and Freedom*, in *Washington and Lee Law Review*, 25, 1, 1968, 166.

<sup>85</sup> Opening Remarks by Ms. Navi Pillay, United Nations High Commissioner for Human Rights to the Side-event at the 24th session of the UN Human Rights Council *How to safeguard the right to privacy in the digital age?*, 20 September 2013, <https://bit.ly/3wPuNDw>, (last visited 12/01/2021); Opening Remarks by Ms. Navi Pillay United Nations High Commissioner for Human Rights to the Expert Seminar: *The right to privacy in the digital age*, 24 February 2014, Room XXI, Palais des Nations, Geneva, <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14276&LangID=E>, (last visited 12/01/2021).

<sup>86</sup> General Assembly of the United Nations, Resolution A/RES/68/167, 21 January 2014, *The Right to Privacy in the Digital Age*, <http://undocs.org/A/RES/68/167>, (last visited 12/01/2021).

<sup>87</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 04/05/2016, 1.

enforcement authorities can access AI systems. This lack of clarity about who is using such tools and for what purposes likewise endangered the application of the transparency principle. The lack of a clear framework for allocating responsibilities, as outlined above, in the use of AI algorithms for public affairs contributes to this opaque situation. It is also not possible to understand *ex-ante* the importance of algorithmic results in the decision-making process of actors such law-enforcement agencies or border guards.

The fairness principle is the crucial core of the relationship between controllers and data subjects.<sup>88</sup> It requires that processing data procedures shall be carried on in a way people could reasonably expect.<sup>89</sup> Algorithms may produce discriminatory results for specific individuals or categories of people in case of biased datasets. This prevents compliance with the fairness principle. However, reliable algorithms must take into account peculiar factors and variables while performing their tasks. An algorithm that produces standardized results without taking variables into account would be almost useless, if not harmful.<sup>90</sup> A fair algorithm should work taking into account such differences without exacerbating discriminatory trends. Nevertheless, the difference between taking every element into account and producing discriminatory results is particularly subtle in sensitive contexts such as migration management. Artificial Intelligence is not a neutral technology. Thus, its deployment could be influenced by the interests at stake.

Machine learning algorithms require more and more data to improve their functioning. However, this need makes it difficult to apply the principle of data minimization stated in the GDPR (Art.5). According to the GDPR, controllers must only collect and process the amount of data that is strictly necessary to achieve their objectives. The principle of purpose limitation (Art.5) is equally endangered by the operation of algorithms in the migration context. According to this rule, controllers can collect data only for purposes previously fixed. The continuous demand for new data means that algorithms do not need information only for predetermined purposes. As far as the migration context is concerned, it should be noted that several actors have access to artificial intelligence tools, as previously explained. Thus, it may be not possible to identify all the interests at stake. More specifically, the use of Artificial Intelligence systems at the borders of the European Union responds both to the need to manage migratory flows and to fight criminal phenomena.<sup>91</sup> For example, law enforcement agencies may use the data collected for administrative purposes, such as issuing an entry visa, to conduct criminal investigations. The Court of Justice of the European Union has clarified that limits must be set to the ability of public bodies to access citizens' data.<sup>92</sup>

---

<sup>88</sup> European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law*, <https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition>, (last visited 24/03/2021).

<sup>89</sup> C. BLASI CASAGRAN, *op.cit.*, 443.

<sup>90</sup> R. BENJAMIN, *Assessing risk, automating racism*, in *Science*, 366, 6464, 2019, 421.

<sup>91</sup> C. BLASI CASAGRAN, *op. cit.*, 446.

<sup>92</sup> Court of Justice of the European Union, Judgement of 8 April 2014, *Digital Rights v. Ireland*, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.



### 6.3. AI-driven border controls and the application of the *non-refoulement* principle

Artificial intelligence tools can contribute to practices of deportation and expulsion of migrants, despite the principle of *non-refoulement* enshrined in international law. According to Article 33 of the Geneva Convention, States cannot expel or return refugees to a territory where their life could be endangered by a risk of persecution.<sup>93</sup> Article 4 of the ECHR prohibits subjecting any person to inhuman or degrading treatment. Article 18 of the same document affirms the right to asylum in accordance with the Geneva Convention relating to the Status of Refugees, including the principle of non-refoulement. Article 19.2 of the ECHR prohibits the return of a person to a state where there is a well-founded danger to his or her life and integrity.

The principle of *non-refoulement* also entails rejection procedures at national borders.<sup>94</sup> Similarly, UNHCR stated that the scope of application of the principle of non-refoulement concerns the national territory, its borders and the high seas.<sup>95</sup> Thus, it applies also to border control procedures.<sup>96</sup> Border guards could use AI tools to identify and intercept individuals approaching the national frontiers and then returning them to their country of origin, regardless of any risk of torture and reprisals they can suffer over there.<sup>97</sup> According to the Eurosur regulation, there cannot be an exchange of information with a third country that could use such data to identify certain persons who have applied for international protection or who are at risk of inhuman and degrading treatment (Art.20). Despite this prediction, studies have shown that European countries rarely carry out thorough investigations to assess whether such risks exist.<sup>98</sup>

## 7. Procedural safeguards in AI-driven individual expulsion proceedings

According to international human rights law, States are required to provide appropriate remedies for individuals who suffer violations of their fundamental rights.<sup>99</sup> As far as deportation procedures are concerned, States shall formulate adequate safeguards for the rights of people involved.<sup>100</sup> More specifically, individuals have the right to appeal against the deportation decision and thus to request stricter scrutiny of this procedure.

<sup>93</sup> Convention and protocol relating to the status of refugee, <https://www.unhcr.org/3b66c2aa10>, (last visited 24/03/2021).

<sup>94</sup> G.S. GOODWIN-GILL, J. MCADAM, *The refugee in International Law*, Oxford, 2007, 208.

<sup>95</sup> UNHCR Note on the Principle of Non-Refoulement, November 1997, <https://www.refworld.org/docid/438c6d972.html>, (last visited 24/03/2021).

<sup>96</sup> Art 2 of the Regulation (EU) No 1052/2013 implementing the EUROSUR system.

<sup>97</sup> A. BEDUSCHI, *op.cit.*

<sup>98</sup> European Union Agency for Fundamental Rights, *How the Eurosur Regulation affects fundamental rights*, [https://fra.europa.eu/sites/default/files/fra\\_uploads/fra-2018-eurosur-regulation-fundamental-rights-im-pact\\_en.pdf](https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-eurosur-regulation-fundamental-rights-im-pact_en.pdf), (last visited 24/03/2021).

<sup>99</sup> Resolution adopted by the General Assembly on 16 December 2005, *Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law*, A/RES/60/147, <https://undocs.org/en/A/RES/60/147>, (last visited 25/03/2021).

<sup>100</sup> Human Rights Committee, *Ahani v. Canada*, Communication n. 1051/2002, <https://juris.ohchr.org/Search/Details/1108>, (last visited 25/03/2021).



Art.22 of the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (ICRMW) prescribes a non-exhaustive list of possible remedies.<sup>101</sup> It includes measures like communicating the deportation decision in a language understandable for people involved and, if possible, in a written form. Furthermore, aliens under expulsion procedure should be able to express their reasons. Protocol n.7 of the ECHR formulates similar procedural safeguards for the fundamental rights of people involved in expulsion proceedings. However, individuals can be expelled without expressing their reasons in the case of national security matters.

The use of artificial intelligence systems to carry out border controls may undermine the effective application of these remedies and safeguards. The black box barrier could prevent border guards and administrative officers to fully explain the reasons behind their decisions. Thus, migrants involved could not submit an appeal against expulsion or rejection proceedings based on algorithmic outputs. The lack of appropriate oversight mechanisms for the use of AI systems in the migration context may therefore render the procedural safeguards just explained essentially inapplicable.

## 8. Concluding remarks and recommendations

The deployment of AI tools in the migration management context is nowadays a well-established practice. Algorithms can perform different tasks, from assessing migrants' applications to individuate the better spots to relocate them. However, relying acritically on the AI potentialities in such a sensible context may represent a mistake from a political perspective and a threat to the fundamental rights of all the people involved.

This paper points out the critical issues and the legal challenges of using AI algorithms to perform border controls, identity checks and other activities related to the management of migration flows. More specifically, this study questions how the inherent features of AI algorithms could be not compatible with the use of such systems in the migration context. It then takes into account factors such as the inherent opacity of algorithmic reasoning, the possibility of replicating and amplifying discriminatory practices, and the lack of a clear liability framework to understand what the problems may be in using AI algorithms in the migration context. These factors can have a potentially devastating impact on the lives of migrants, refugees and asylum seekers.

The ill-considered and not carefully regulated use of algorithmic tools in such a sensitive context as migration can lead to the non-respect of fundamental principles such as equality and non-discrimination. It can cause the infringement of the privacy and data protection rights of those involved in the above explained algorithmic controls. Border rejections and deportation measures based on algorithmic outputs may violate the principle of non-refoulement and condemn migrants to take intolerable risks to their lives and safety.

This paper looks at the measures implemented by the European Union in the field of algorithmic controls in the context of migration to understand whether European decision-makers have taken into account these possible risks for the fundamental rights of migrants, refugees and asylum seekers.

---

<sup>101</sup> International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families adopted by General Assembly resolution 45/158 of 18 December 1990, <https://www.ohchr.org/en/professionalinterest/pages/cmw.aspx>, (last visited 25/03/2021).



The iBorderCtrl project funded by the European Commission is a clear example of how the use of algorithmic systems at European borders can have worrying results and create dystopian situations. The AI-driven lie-detection system was responsible for checking the reliability and truthfulness of travelers' statements at border controls to enter European territory. However, the functioning of this mechanism was obscure and not understandable to human observers. There was also a risk that it would take into account variables such as the ethnic origin or nationality of respondents in a discriminatory manner.

The iBorderCtrl case illustrates how algorithmic technologies are not inherently neutral, but they act accordingly to purposes determined by actors and stakeholders. As far as fields of public importance like migration management are concerned, elected politicians and lawmakers formulate such purposes.

The migration crisis of 2015 and the gradual rise to political power of parties that see immigration as a possible threat has influenced European action. The EU is currently funding the implementation surveillance tools and training programmes for border police in neighbouring countries.<sup>102</sup> The aim is to prevent migratory flows currently in circulation from reaching EU territory.

This attempt to "outsource" the surveillance of European borders and the management of migratory phenomena to other States raises several concerns. All the more so considering the impact that algorithmic tools can have in such a situation, as explained in this paper. Several EU bodies and agencies are funding these activities for different goals and acting on different legal grounds. The lack of a clear framework of intervention for these programmes is an issue in terms of fundamental rights safeguards. The EU's increasing focus on the technological control of its borders has led to an increase in the budget for Frontex.<sup>103</sup> Similarly, surveillance systems industries are constantly lobbying Frontex officers to influence their actions and therefore increasing their profit opportunities.<sup>104</sup>

Thus, private economic interests and political pressures can be determining factors in influencing EU action in managing migration phenomena.

The EU Member States must cooperate to develop an integrated and collaborative border management policy (Art.77.2 TFEU).<sup>105</sup> The principles of solidarity and fair sharing of responsibilities must characterize the European Union's action in the context of migration and management of its borders (Art.80 TFEU), including the deployment of technological means at the European frontiers.

The European Parliament recently did not approve the financial budget of Frontex over concerns about the lack of respect for fundamental rights in the management of migratory flows.<sup>106</sup>

<sup>102</sup> Privacy International report, *Borders without borders: how the EU is exporting surveillance in bid to outsource border controls*, <https://privacyinternational.org/long-read/4288/borders-without-borders-how-eu-exporting-surveillance-bid-outsource-its-border>, (last visited 26/03/2021).

<sup>103</sup> Statewatch, EU: Frontex splashes out: millions of euros for new technology and equipment, 19/06/2020, <https://www.statewatch.org/news/2020/june/eu-frontex-splashes-out-millions-of-euros-for-new-technology-and-equipment/>, (last visited 26/03/2021).

<sup>104</sup> M. Douo et al., *Lobbying fortress Europe. The making of a border-industrial complex*, in *Corporate Europe Observatory*, 05/02/2021, <https://corporateeurope.org/en/lobbying-fortress-europe>, (last visited 26/03/2021).

<sup>105</sup> Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26/10/2012, 47.

<sup>106</sup> Press release, *EU refuses to approve Frontex's budget over human rights concerns*, in *Al Jazeera*, 23/03/2021, <https://www.aljazeera.com/economy/2021/3/23/eu-refuses-to-sign-off-on-frontex-budget-over-human-rights-issues>, (last visited 29/03/2021).



In conclusion, this paper is intended to point out the several risk factors for the fundamental rights frameworks of using AI tools in the migration context without considering the consequences. AI algorithms can produce biased outcomes which serve as legitimate grounds for discriminatory policies. Thus, this paper argues that oversight mechanisms are needed. Independent authorities should periodically check the functionality and fairness of AI algorithms deployed at the European frontiers. Humans must be able to understand and question the algorithmic outcomes before using them in their decision-making process. Migrants, refugees and asylum seekers should likewise be aware of such process and be able to appeal final decisions in case of an alleged violation of their rights.

Migration management is a field involving political influences and economic interests carried on by private parties, as outlined above. The European Union should finance only technologically border surveillance programmes providing for a clear governance framework. Public institutions must carry on severe scrutiny on the implementation of such procedures to ensure compliance with the human right framework. They must investigate in-depth the algorithms employed for migration management purposes to detect potential biases and to understand their reasoning process as much as technologically possible. Thus, they should choose algorithms which are not showing an unsurmountable black-box barrier, if possible.

Public bodies should establish a constant dialogue with surveillance tools suppliers and AI providers to make the algorithms fundamental rights compliant, regardless of proprietary issues. More specifically, public bodies must tell AI manufacturers which values algorithms should follow in their working routine according to their political views. However, continuous public control should check the fair implementation of these decisions. In other words, democratically elected bodies should decide public policies instead of private business-oriented entities, like surveillance tools industries or AI providers.

As far as migration management is concerned, public bodies must decide which interpretation of chosen values AI algorithms should follow according to the peculiarities of this field. The concept of privacy has different meanings depending on social, cultural and geographical contexts.<sup>107</sup> AI algorithms must therefore take into account cultural differences in managing migration flows composed of people coming from several different backgrounds into the “Western” European territory. Frontex should therefore provide an adequate training programme for its personnel on the functioning of AI-driven border controls and about the cultural divergencies in terms of privacy and data protection to assist migrants, refugees and asylum seekers through identification policies.

An AI-driven migration management policy is possible, but human intervention is still necessary to safeguard the fundamental rights framework.

---

<sup>107</sup> L.A. BYGRAVE, *Privacy and data protection in an international perspective*, cit.