**Impact of digital technology on discriminatory policies in the border management**

**Submitted to**: The Special Rapporteur on contemporary forms of racism

**Submitted by**: Maat for Peace, Development and Human Rights, (an organization with in special consultative status with the United Nations Economic and Social Council).

**Submitted in**: May 2020

* **Digital techniques in border enforcement and administration... models, context and relevant actors.**

Countries are adapting internal immigration laws, with the aim of using a set of methods and technologies that prevent illegal entry of undocumented aliens. These methods vary from one country to another. Some countries are patrolling their borders, building walls along the borders, or making use of intelligence applications such as biometric technology, big data analysis, algorithms, decision-making tools, machine learning programs, and predictive analysis. However, these methods are sometimes accompanied by severe human rights violations such as discrimination and racism, especially against migrants, refugees, and stateless persons.

In this light, various countries have recently relied on a variety of artificial intelligence applications to secure their borders and counter the illegal influx of refugees and immigrants. In the United States of America, biometrics technology is used in the context of border management as an artificial intelligence application that recognizes the measurable physical and behavioral characteristics of people, therefore, allowing security agencies to identify and verify an individual's identity. Biometrics can be defined as the process by which the person’s physical features and characteristics are detected and registered by an electronic device or system as a way to verify identity. In this context, Germany uses digital fingerprint capture technology, which is part of biometrics, in order to register and receive refugees; therefore, it has a reliable database about them.[[1]](#footnote-1) It is worth noting that biometrics techniques are highly effective for identification in border management use cases because they leverage biologically unique traits (such as: fingerprints and face) to decisively identify individuals trying to enter the country illegally and counter them.[[2]](#footnote-2)

In the light of the increasing influx of refugee numbers to Europe due to the Syrian crisis that began in 2011, a number of European countries used the "automated-decision making" technique to prevent refugees from crossing into their country. The automatic decision-making process indicates a form of automated processing of personal data in which personal data are used not only to evaluate certain personal aspects of a natural person, but also to analyze or predict aspects of that person's performance at work, his economic situation, health, personal preferences, interests, reliability, behavior, location, or movements. All personal data are collected through a variety of sources. Organizations, for example, obtain personal information about individuals from a variety of different sources, such as Internet searches of individuals, their purchasing habits, and lifestyle and behavior data collected from mobile phones, social networks, video surveillance systems and the Internet. Switzerland, Canada, and Britain adopt this method for selecting refugees and resettling them in their country[[3]](#footnote-3).

In this context, the American technology company Unisys that provides information services, technology, and software, develops Artificial Intelligence solutions and services to help the U.S. Government controlling and managing its border through assessing a wide range of metrics in determining whether a traveler seeking to enter a country poses a security threat. It is worth noting that the company itself has highlighted its work in constructing the Australian Department of Immigration and Border Protection’s biometric system, as well as other activities in the service of European Union and CBP border control programs.[[4]](#footnote-4)

In Canada, various data analyzes are used in the management of migration and asylum seeking processes. Data analyzes indicate the use of information technology to leverage statistics, algorithms and other mathematics tools to improve decision-making processes regarding immigration and asylum applications[[5]](#footnote-5). While the European Union and the United States of America use lie detection technology to examine travelers and monitor different borders using specific AI-based algorithms that contribute to capturing illegal immigrants, preventing cross-border crimes and combating terrorism.[[6]](#footnote-6)

In this context, it is mentioned that there is a group of cultural, historical and political factors that led to the use of technology, especially artificial intelligence techniques, in controlling borders to prevent people from crossing them illegally, among which is the spread of terrorist threats to the national security of countries. In the United States of America, a system of biometric technologies has been adopted after the terrorist attacks of September 11, 2001 in 2001 as a result of protecting the state from the threat of terrorism, especially the threat posed by the Middle East. In response to that, the US Congress enacted a set of laws that require a wider use of biometrics in Border surveillance systems to curb the effects of terrorism.[[7]](#footnote-7)

In the United States of America, as well, increased security concerns resulting from the growth of transnational crime and terrorism have increased interest and research in the potential of biometric technology to carry out cross-border identity checks. It is worth noting that biometrics receives a great deal of attention as a means to bridge gaps in traditional border control methods. Measurements are the physiological or behavioral characteristics used to identify or verify the identity of a living person, and physiological characteristics include fingerprints, hand geometry, iris shape, face, sound, ear shape, and body odor. Behavioral characteristics include handwritten signatures and the way a person walks. Any kind of this biometric information may allow guards to detect and investigate identities faster, and then prevent terrorists from entering the country.[[8]](#footnote-8)

In addition to the growing threat of terrorism to the national security of countries, political and security crises and civil wars in the Middle East have taken place since 2011 until now, causing more illegal refugees to enter the European Union, which have taken a set of measures to let refugees in, especially those from Syria and Yemen. Programs such as the European Border Control System (EUROSUR) and Frontex are examples of information and communication technology (ICT) surveillance where big data technologies are increasingly used to predict, control and monitor traffic across European Union borders.[[9]](#footnote-9)

* **The discriminatory effects of using digital technologies in the context of border enforcement and management.**

The use of artificial intelligence techniques in the context of border control has many negative effects on the rights of migrants, refugees and stateless persons, for example in the “automated-decision making” technique that analyzes the applications of immigration and asylum applicants, data errors may occur leading to the rejection of immigration requests. Canada uses automated decision-making systems for immigration applications which contribute to discrimination against immigrants, non-citizenship residents, and other vulnerable persons due to the mechanisms by which automatic decision technology works to reject these people. It is worth noting that the algorithms upon which programs rely is not neutral in any way, as it is a set of guidelines based on the analysis of previous data that is used to teach the apparatus how to make a decision, because the machine does not think or understand the decision it makes and does not take into account the human dimensions, causing human rights violations and discrimination against some people in this regard.[[10]](#footnote-10)

In this context, the capabilities of biometric technology do not allow individuals to select the data preferred to be registered or used, which violates the individual’s cultural and religious habits, nor does it allow informed consent, violating the moral right of integrity. In the same vein, biometric measurement models lack vital policies, procedures, and ethical guidelines for collecting and processing data or may allow individuals to process data without permission, which sometimes violates the right of individual to freedom. Moreover, children's lack of knowledge of artificial intelligence monitoring systems and techniques contributes to violating children's rights who are discriminated against due to their poor knowledge of such systems. Additionally, these systems do not take into account the social traditions and family life.[[11]](#footnote-11)

Automated decision-making systems used to monitor borders in Canada perpetuate different stereotypes about immigrant women, promoting racial discrimination against them and, consequently, leading to more discrimination against gays, clergy men, and some other groups and minorities, which are mostly racial biases based on signs of stereotypical appearance related to gender, clothing, or culture while assessing refugee applications, these systems do not take into account the weaknesses and overlapping identities, that part of which may be attributed to community-related issues such as women's flee from domestic violence or racial discrimination against LGBT people. Notably, the use of discriminatory and biased algorithms has profound consequences on the integrity of the human being, his life, freedom and security. It impedes human migration, reducing it to a mere set of variables due to the nature of a particular software program.[[12]](#footnote-12)

In this context, the United States of America has developed a program called “Extreme” to audit initiatives in immigration management, in order to predict the behavior of people who aim to enter the United States of America and to predict whether they intend to commit criminal or terrorist acts after allowed into the country. Considering the different sides of this method reveals that it prohibits travel from seven Muslim-majority countries to the United States: Syria, Iraq, Iran, Libya, Somalia, Sudan, and Yemen. Besides, it allows access to government agency databases, law enforcement, and collecting data from public information available on the internet and social media platforms, through the relevant tools of artificial intelligence technologies. All this information will be analyzed constantly to check travelers during their existence in the United States, leading to serious discrimination against some Muslims who are considered and treated as terrorists, a truly unforgivable mistake. This, is in addition to perpetuating the stereotype of a Muslim as a terrorist, violating the cultural and religious rights of Muslims[[13]](#footnote-13).

In May 2018, the U.S. Immigration and Customs Enforcement (ICE) stated that it was taking severe measures in monitoring the immigrants and refugees social media content in the context of collecting various information for immigration management programs, while the administration was using the same set of discriminating criteria to receive refugees and immigration applicants from countries with Islamic backgrounds that are referred to in the previous ban Act[[14]](#footnote-14). In this context, Australia’s border authorities has rolled out an entirely automatic, seamless processing system for incoming passengers based solely on their biometric data such as fingerprints, iris and facial recognition, causing racial discrimination against some of them.[[15]](#footnote-15)

In this framework, discriminatory practices deeply entrenched in the use of machine learning may affect individual’s immigration decisions and their freedom of religion and expression, by affecting the freedom of movement of citizens and the right to travel. These non-transparent systems may indicate early deportation and prevent individuals from obtaining a valid visa to stay in a country. In 2017, the New Zealand Immigration Department began introducing a system that uses age, gender, and ethnicity of immigrants to identify potential rioters, perpetuating racial discrimination against immigrants.[[16]](#footnote-16)

While European Union countries use smartphone data as a weapon to deport refugees and reduce their number, as Germany and Denmark have expanded the laws that enabled immigration officials to extract data from asylum seekers’ phones through various artificial intelligence applications[[17]](#footnote-17), and in Britain 7,000 students were wrongly deported because a wrong algorithm accused them of cheating in language acquisition test, indicating the unfair deportation of people based on wrong data. In the United States of America, the Immigration and Customs Enforcement Agency has partnered with Palantir Technologies to follow and separate families as well as to deport and detain persons fleeing violence from Central and Latin America, based on a range of different applications that support artificial intelligence in border control.[[18]](#footnote-18)

  It is worth noting that Palantir Technologies has provided the American Agency with the technology that supports detention and deportation programs run by the US Immigration and Customs Administration, which rely on artificial intelligence technologies that contributed to the violations of the rights of migrants and refugees, while the use of artificial intelligence-based surveillance techniques along the Mexico-U.S. border has a three-fold greater mortality rate, with immigrants being pushed toward more dangerous routes across the Arizona desert. Automated decision-making biases are widely documented in immigration management. These biases have far-reaching consequences if included in the emerging migration techniques. In airports in Hungary, Latvia, and Greece, a new project by a company called iBorderCtrl has been introduced. This project contain lie detectors operating by artificial intelligence at border checkpoints, and it can contribute to the prejudices imposed on humans.[[19]](#footnote-19)

While the United Nations relies on filling its databases with biometrics and collecting biological data from over 8 million people, most of whom are fleeing conflict or need humanitarian assistance, which sometimes violates the individuals’ rights and freedoms and aggravates the risk of repression by authoritarian governments that control conflicts. For example, in the case of collecting biometrics data from Rohingya refugees in Myanmar, the so-called refugee data details could facilitate defining repressive governments, identifying groups and taking them out of camps. China has also used facial recognition to track and locate the Uighur Muslim minority[[20]](#footnote-20).

**Conclusion & Recommendations**

Eventually, it can be said that the use of artificial intelligence applications such as biometrics, the big data analysis and algorithms, the decision-making tools, the machine learning programs and the predictive analysis in managing border areas to prevent the flow of illegal immigration may lead to widespread violations of the rights of refugees, migrants and stateless person, causing racial discrimination, excluding immigration and deportation requests, violating privacy for individuals and violating the principles of informed consent in some cases. Therefore, **Maat for Peace, Development and Human Rights** recommends the following:

* Biometrics for border control should provide information about what and why biometrics are used in addition to allowing selection policies and procedures unless selection is not applicable.
* Biometrics for border control must include a set of free and informed consent of individuals in accordance with the rules established by the principles of international law and human rights conventions.
* Biometrics for border control must apply a policy to restrict the procedures of collecting and processing data, and striking a balance between legal interest and personal freedom.
* Biometrics for border control should envisage the adoption of devices and procedures to ensure that children are treated well.
* Biometrics for border control must include a non-discrimination policy that is consistent with human rights legislation, in a way that prevents various biases.
* Biometrics for border control must adopt appropriate measures for family approval and procedures.
* Biometrics for controlling border security must be guaranteed to ensure confidentiality, integrity, availability, and constant flexibility of treatment systems and services.
* There must be a set of legal mechanisms allowing asylum-seekers to complain against errors made by artificial intelligence technologies.
* Double principles ranging between relying on artificial intelligence techniques and human beings must be adopted to avoid different biases in this framework.
1. Special Report: Biometrics and Border Security. .scribd. Jun, 2016. <https://bit.ly/2zjXmjV> [↑](#footnote-ref-1)
2. Biometric identification in border management. Aware. <https://bit.ly/3bDrjK0> [↑](#footnote-ref-2)
3. Data & Algorithms for immigration control: unravelling the iceberg of automated-decision making. Medium. November , 2019 <https://bit.ly/2S6cnfN> [↑](#footnote-ref-3)
4. Unisys Software Brings Machine-Learning AI to Border Control . findbiometrics. March , 2018 <https://bit.ly/34ZHqzh> [↑](#footnote-ref-4)
5. Data analysis for effective border management – the Canadian experience. .wcoomd. <https://bit.ly/3eMfrYj> [↑](#footnote-ref-5)
6. The science behind the EU's creepy new border tech is totally flawed. Wired. November 2018. <https://bit.ly/2VTA5Nw> [↑](#footnote-ref-6)
7. TechnologyAssessment Technology Asse ssmentUsing Biometricsfor Border SecurityUsing Biometricsfor Border Security .United States General Accounting Office. November 2002 <https://bit.ly/2VS2d3u> [↑](#footnote-ref-7)
8. Biometrics, Migrants, and Human Rights. Migrationpolicy. MARCH 2005. <https://bit.ly/2Kx9osA> [↑](#footnote-ref-8)
9. Augmented borders: Big Data and the ethics of immigration control. Researchgate. March 2015. <https://bit.ly/3eKQhZX> [↑](#footnote-ref-9)
10. Immigration decision-making: Artificial Intelligence may violate human rights. Setzer Immigration Law. <https://bit.ly/2KvSKcX> [↑](#footnote-ref-10)
11. How to Do It Right: A Framework for Biometrics Supported Border Control. springer. December 2019 <https://bit.ly/3eMyW2X> [↑](#footnote-ref-11)
12. Bots at the Gate A Human Rights Analysis of Automated Decision Making in Canada’s Immigration and Refugee System. Citizenlab . 2018 . <https://bit.ly/2yLfiDJ> [↑](#footnote-ref-12)
13. Executive Order Protecting the Nation from Foreign Terrorist Entry into the United States. Whitehouse. January, 2017. <https://bit.ly/2S7ZguK> [↑](#footnote-ref-13)
14. Bots at the Gate A Human Rights Analysis of Automated Decision Making in Canada’s Immigration and Refugee System مرجع سابق ذكره [↑](#footnote-ref-14)
15. Facial recognition to replace passports in security overhaul at Australian airports. Theguardian. <https://bit.ly/2Y20w6h> [↑](#footnote-ref-15)
16. Bots at the Gate A Human Rights Analysis of Automated Decision Making in Canada’s Immigration and Refugee System مرجع سابق ذكره [↑](#footnote-ref-16)
17. Europe is using smartphone data as a weapon to deport refugees. Wired. July 2018. <https://bit.ly/2XXVyrg> [↑](#footnote-ref-17)
18. The human rights impacts of migration control technologies . edri. Feb 2020https://bit.ly/3ePbIJu [↑](#footnote-ref-18)
19. Emerging Voices: Immigration, Iris-Scanning and iBorderCTRL–The Human Rights Impacts of Technological Experiments in Migration . opiniojuris. <https://bit.ly/2KwRQNk> [↑](#footnote-ref-19)
20. Technology on the margins: AI and global migration management from a human rights perspective. Cambridge International Law Journal. 2019 <https://bit.ly/3aCnlQF> [↑](#footnote-ref-20)