Expert contribution to the report on the Externalization of Migration and the Impact on the Human Rights of Migrants

Author: Marianna Poyares, Ph.D., on behalf of the **Center on Privacy and Technology at Georgetown Law, Georgetown University**

Our contribution focuses on two specific examples of border externalization through the use of digital technologies. First, I will outline how the unwarranted extraction of migrants' DNA by the United States Department of Homeland Security, and, second, the provision of education services by the International Rescue Committee (IRC) in partnership with OpenAI in humanitarian settings. These are two dramatically different examples of border externalization carried out by different agents for different purposes. The first, the extraction of non-citizen DNA carried out by the United States Department of Homeland (DHS) Security has become a standard practice since 2020, and it is carried out either by Customs and Border Patrol during cross-border encounters, or by Immigration and Customs Enforcement within the national territory. DHS claims the practice, frequently carried out without knowledge or consent from the migrant, aims at strengthening national security by making genetic profiles of non-citizens available for future policing both at the domestic level as well as internationally. The second example, namely the use of virtual platforms and chatbots for the provision of educational services by the International Rescue Committee through the AprendIA program, is the result of a partnership with OpenAI. AprendIA is one example among many others of the quickly-expanding partnership between humanitarianism and Big Tech, where digital service outreach is expanded at the cost of dwindling transparency and scarce accountability for user data and rights protections. These two examples stand as paradigmatic of what Poyares calls "migrant data extractivism" (Poyares, "Migrant data extractivism: tech and border at the limit of rights", *International Migration, an IOM Journal.* forthcoming), namely a new economy that operates through border externalization and that preys upon the vulnerability experienced by forcibly displaced persons for expanding, without public oversight, rampant extraction of user data with considerable behaviour-predictive value, and profiling securitization technologies.

Case # 1- DNA extraction of non-citizens by the United States Department of Homeland Security.

(all information below in addition to supporting material and primary research can be found in Glaberson, Tse, and Tucker. *Raiding the Genome: How the United States Government is Abusing its Immigration Powers to Amass DNA for Future Policing.* Center on Privacy and Technology at Georgetown Law)

Summary:

In 2019, the United States Department of Justice (DOJ) introduced a new rule to remove key exceptions in the regulations that govern DNA collection by DHS. The new rule, which went into effect in 2020, requires the agency to take DNA from anyone the agency detains, even very briefly. As neither the 2020 DOJ Rule nor the underlying statute define the kinds of detention that can authorize DNA collection, DHS has been utilizing the full extension of its discretionary power to detain immigrants to perform DNA

collection. This includes situations that range from an interview in an airport room, a credible fear screening with a border patrol agent, being pulled over by a CBP officer when approaching the territorial border by car, to being processed by ICE in a detention facility. “DHS now takes DNA from hundreds of people every day and sends those samples to the FBI to be added to the Combined DNA Index System (CODIS), a network of biometric databases accessible by law enforcement agencies all over the United States” (Glaberson, Tse and Tucker, p.8), as well as to partner international law enforcement agencies. Before the 2020 rule almost all DNA profiles included in the CODIS database were gathered by state and local police officers through the criminal legal system. Between 2020-2024, DHS alone has been responsible for adding more than 1.5 million new genetic profiles to CODIS, including that of a 4-year old.

All profiles added to CODIS are stored under the database “offender” index, even those collected by DHS which were extracted without any of the procedural rules that law enforcement must follow when taking a person’s DNA sample. Once a profile is added to the database, it is held in perpetuity (both the biological sample and the digital profile). According to the *Raiding the Genome* report, “even though DHS’s internal policies require ICE and CBP officials to inform people before taking their DNA, many people we interviewed were not aware their DNA had been collected or thought the swab was for the purpose of a COVID-19 test. Those who were aware of the collection submitted to a cheek swab under threat of criminal prosecution if they did not comply.” (Idem, p.3) Furthermore, given the demographic makeup of people coming to the United States that are stopped by ICE and CBP, DHS’ addition to CODIS disproportionally target black and brown immigrants which means that, in practice DHS migrant data collection stands as a broad-scale practice of racial profiling and criminalization of migrants of colour that extends beyond the jurisdiction of the territory of the United States.

Use of technology:

DNA samples are collected by DHS agents (either Customs and Border Patrol or Immigration and Customs ENforcement) through cheek swabs that are subsequently stored in a closed vial. The vial is sent to the FBI where it is processed by forensic scientists and a digital profile is created and added to the CODIS database. Both the CODIS “offender” digital profile and the biological sample are kept, in perpetuity, in the possession of the FBI. The “offender” biometric profile is shared, through CODIS, with more than 58 international law enforcement agencies, according to the FBI.

Human rights implications:

Once an individual’s biometric profile is added to CODIS, there are no instruments for recourse, either at the national or the international level. Migrants, including those under humanitarian parole, are coerced into having their DNA extracted at the cost of either being denied entry and protection, or facing criminal charges of impeding migration enforcement–refusal to comply with DNA extraction makes a class A misdemeanor punishable by up to one year in prison.

Considering the highly sensitive nature of genetic identification, it is crucial to highlight that a profile added to CODIS is capable of identifying not only the original migrant whose genetic sample was extracted but also close relatives, including unborn offspring. This means that the profiling and criminalization of vulnerable migrants, especially migrants of color through the extraction of genetic material and the subsequent addition of the genetic digital profile to a criminal law database under the label "offender" may very well target relatives of the original individual. According to Glaberson, Tse, and Tucker, "federal officials are on record stating their interest in keeping these samples precisely so that they can use them in conjunction with future-developed technologies. Our research uncovered a number of such technologies with which law enforcement officials nationwide are toying, from robust profiles called "single nucleotide polymorphisms" or "SNPs" (pronounced "snips") that can allow law enforcement agents to "rummage around" in people's family trees, to locally-controlled "rogue" DNA databases, to "daisy-chaining" together dangerous and untested tools. Current law is insufficient to protect against the risk that future administrations might mine DHS-collected DNA samples in order to target vulnerable communities". (idem, p.5)

This is not only an unprecedented extrapolation of pre-crime profiling as well as its extension into future generations. There are no provisions, statutes or instruments that provide migrants and their families access to justice in the case of human rights violations that occur either in the course of the procedure of DNA extraction and criminal profiling, or that may arise as a result of it.

Legal framework:

DHS migrant DNA extraction and migrant criminal profiling is supported by the 2019 (effective 2020) DOJ rule DNA-Sample Collection from Immigration Detainees, 85 Fed. Reg. 13,483 (Mar. 9, 2020) (codified at 28 C.F.R. § 28.12). However, the practice goes against a number of principles listed in the 1997 Universal Declaration on the Human Genome and Human Rights, and its subsequent Guidelines for the implementation (issued on 16 November 1999 by 30 C/Resolution 23), both endorsed by the United States. This includes the special status of human genetic data, and institutes that the collection, processing, and storage of human DNA for civil legal preceding (as well as criminal) must be consistent with international human rights law. Furthermore, DHS extraction of migrant DNA without individualized suspicion of criminal wrongdoing violates the Fourth Amendment to the United States Constitution.

Case #2 - International Rescue Committee's (in partnership with OpenAI) AprendIA program

(all information below in addition to supporting material and primary research can be found in Poyares, "Migrant data extractivism: tech and border at the limit of rights", *International Migration, an IOM Journal.* forthcoming)

Summary:

The International Rescue Committee's AprendIA program as an example of how partnerships between Big Tech and NGOs for the provision of services for forcibly displaced persons under humanitarian

protection may operate by circumventing human rights protections, preying onto a scenario of forced immobility and scarcity for extracting and mining migrant data. AprendIA is an "AI-driven chatbot platform that delivers educational and training experience to learners through messaging platforms" (www.aprendia.io). In a global context where almost 200 million forcibly displaced children do not have access to quality education, the program addresses a crucial infrastructural void left behind by local state authorities, namely, access, as put broadly by the project's description, to "educational experiences". IRC's initial public communication (IRC, 2024) emphasizes the 225,000 dollars award from OpenAI driving the project, its main target of creating a platform for supporting and providing educational material for teachers and learning facilitators (such as parents), and the initial pilots in Nigeria, Colombia, and Bangladesh. What sets AprendIA apart is providing access to a chatbot for support in situations of forced displacement. "Integrating Generative AI through OpenAI's ChatGPT, we personalize the experience, making it responsive to the unique needs of educators, and ensure quick adaptation to new contexts for rapid deployment during acute emergencies" (airbel.rescue.org).

While partnerships between Big Tech and the humanitarian sector are established through donations and gifts (of personnel, technology, platform use and/or licences), under the title of 'corporate philanthropy', the whole endeavour is incredibly profitable for the companies. These "philanthropic partnerships" only happen at the expense of mining data from the "serviced" populations, the generation of data surplus the user provides to the chatbot, the training of algorithms through user interaction and feedback loops. Furthermore, considering that the interaction happens through the mediation of messaging platforms, some of which connected to the users' social media profile, it is unclear how much/what kind of user data is being collected through the interaction with the aprendIA/OpenAI chatbot. Nonetheless, efficiency and easy navigation seem to outweigh concerns regarding potential limits of transaction, extraction, and the chain of custody of one's sensitive and behavioural data.

Human Rights Implications:

Migrant data extraction in contexts of forced immobility through the provision of services by non-state actors in partnership with Big Tech has thrived under purported efficiency even when disregarding transparency, accountability, and human rights protections. Questions include the impossibility of the platform user providing meaningful consent (as the withdrawal of consent implies no access to educational services), no transparency over user data extraction, storage and processing, no oversight mechanisms, lack of standing from the part of the migrant vis-à-vis the non-state actors. It is imperative to highlight that the extraction of sensitive and behavioural data of racialized migrant populations in contexts of immobility that enhance LLM and AI models could reproduce and exacerbate some of the human rights violations listed in the Report for the United Nations Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, *AI and Racial Discrimination in U.S. Border Enforcement*.