

Session Title: "Biometrics and Identity in the Global South"

Date: December 20, 2017

Time: 10:10 - 11:40

Session Organizer: Maria Paz Canales, Derechos Digitales América Latina

Chair/Moderator: Marianne Diaz, Derechos Digitales América Latina

Rapporteur/Notetaker: María Paz Canales, Derechos Digitales América Latina

List of Speakers and their institutional affiliations:

Leandro Ucciferri (ADC, Asociación por los Derechos Civiles)

Martin Borgioli (Hiperderecho)

Smitha Krishna Prasad (Centre for Communication Governance at National Law University Delhi)

Kyung-Sin ("K.S.") Park. (Professor, Korea University Law School)

Olivier Alais (Technologist, independent)

Key Issues raised (1 sentence per issue):

- Lack of transparency in the handling of biometric databases
- Lack of judiciary control over biometric data
- Mandatory enrollment in biometric recognition systems
- Use of biometric data as criminal evidence
- Use of biometric data in immigration controls
- Security standards of biometric databases

If there were presentations during the session, please provide a 1-paragraph summary for each presentation:

Leandro Ucciferri: The Federal System of Biometric Identification in Argentina (SIBIOS) has been used to investigate small crimes, without transparency on which criterias rule the

way information is accessed. The access to information by different governmental bodies does not require warrant. This poses a threat to the presumption of innocence. In the last 5 years there has been a naturalization of use of biometrics, any device produced in this time introduces some biometric functionality. People are not thinking about how this affects them and how this interferes with the exercise of their rights. Another concern is how the biometrics can be used as criminal evidence, because the information is spread without control and biometric cannot be replaced. This is relevant if we think in terms of massive use and collection of biometric.

Martin Borgioli: Biometric data collection has been implemented in Peru for public safety purposes. The legal framework is not respectful of rights. The system was administratively implemented (not by law) and never has been subject to judicial control. Peru has had biometric verification since 20 years ago. In 2006 RENAC (government agency in charge of the biometric register) acquired software to avoid duplication of identity. In 2013 it began to collect facial features as well. These measures were taken to improve commercial transaction security, but without transparency. Today several private actors require biometric verification. Since this year, mobile providers require biometric registration for SIM cards. These providers are forced to provide metadata to police without judicial order. Immigration control also requires biometric data to identify travelers. Biometric is also used as an alternative measure to prison, where people are mandated to register their fingerprints once a month.

Smitha Krishna Prasad: In India the system has been promoted for helping people, but it implies a trade-off between economic rights and privacy rights, while rights should not be traded for any cause. In India, the initial idea to use biometric was proposed in 2009, but didn't pass the control of the parliament. The law only came in 2016 when the Aadhar system had been already administratively implemented, and it was challenged in the court. Since 2013, the Supreme Court has issued orders to avoid the mandatory use of this Aadhar number until its validity is ruled upon, preventing it can be mandatorily required to link bank information, SIM cards registration, welfare providing to children, etc. There is a central database with all this information that is not clear that is secure enough. While there exists a law that makes it illegal to publish Aadhar numbers, there have been several cases of data leak. In 2016 the only leaks prosecuted were the people that reported leaks from authorities. There are many issues of discrimination and exclusion as a consequence of this system: In past October, the press covered the case of a girl that died of starvation because she was not in the register, so she didn't receive welfare food. There is another problem with villagers whose fingerprinters can't be read by the machines. However, in last October, many ecommerce companies started to require Aadhar numbers for tracking packages, even when it is a private company and they don't have authority to require this as mandatory.

Kyung-Sin ("K.S.") Park: Korea has implemented an ID system for every born. The residence registration is a key data that accompanies the person during her whole life. If any criminal has access to the number, then they can access any aspect of the individual. Korea is hit with periodic massive data breaches. The result of this is the lost of agency of people, the system is not reliable enough. The data has two relevant factors for privacy: identifiability and confidentiality. The more identifiable the information, the more privacy

implications. There is a need to think more in this than in confidentiality. The government thinks they are accessing public information, but it is not and it should be required a judicial authorization. It is not only about confidentiality, but rather to control the identity. There is an analogy to unmasking a person and it should be subject to a request. There is a need to take steps in that direction.

Oliver Alais: I have personal experience building a health system in Thailand for immigrants coming from Myanmar, without ID because they are illegal in the majority of cases. They don't have access to healthcare when they arrive in Thailand, so some private clinics tried to help them providing a micro insurance system. They try different systems and they were not working because they were not able to bring technology to rural areas. They had to design a very light solution, because there is no devices or technical skills available. Finally, they realize that just a card with a picture and a code was the most efficient system, giving up the idea of using more sophisticated biometrics. The other problem is the building of the database and where the data of all this information of illegal immigrants is stored. The data has being encrypted, but there is not a real complete solution.

Please describe the Discussions that took place during the workshop session (3 paragraphs):

Discussing good practices in the use of surveillance cameras in public space, KS Park commented that we are born anonymous, because even if you see a face you cannot determine identity, affirming that it should be enough to protect the data by making necessary the use of a warrant to access the data in case of criminal investigations. Leandro disagreed, saying that there is a need to challenge the use of the system in general, to challenge if it even works for addressing the issues that it's supposed to address, because the only thing this technology does is to move the hot spots of crimes in the city. If there is no prove of the affectivity we should push it publically through FOIA. With this is possible to change voters' perspectives.

Discussing the general audience's perspectives and how to approach these perceptions, Martin said that there is a need to educate people and ask government for the information. The government should inform for what the information is used. There is a study that shows the correlation between democratic systems and biometric use. That seems to point out that this is a bigger problem than just education. It is something that needs to be addressed as part of the democratic requirement of government.

After that, we discussed legal limitations on the use of data, through data protection laws that can be used to force government' accountability. There is the need to distinguish between sensitive data and other data in the regulations, because biometric data and other sensitive data pose greater risks. At the same time, we need to have more security obligations in the holding and managing of data ingrained in specific ways in these laws.

Please describe any Participant suggestions regarding the way forward/ potential next steps /key takeaways (3 paragraphs):

There is a need to use more secure systems and to make laws that include standards for secure use and holding of these systems. Meanwhile, in countries like India, where there doesn't even exist data protection laws, it's absolutely urgent to create basic standards for this.

There is an urgent need to educate people about the consequences of use of these biometric systems. There is a need to have more information about why information is collected and how is being used by government. Narrative is pretty strong in keeping people safe and there is a need to overcome it pointing out the risks.

Accountability of governments is necessary for the use of information.

Gender Reporting

Estimate the overall number of the participants present at the session: 7

Estimate the overall number of women present at the session: 3

To what extent did the session discuss gender equality and/or women's empowerment?

While the session didn't have a gender-specific focus, we did comment on the impact of biometrics in groups that are traditionally disadvantaged, which included impoverished people, impoverished women, and LGBTI+ people, with the particular aspect of LGBTI+ bodies being sanctioned and discriminated upon by most of the implementations of biometrics technologies in the countries we discussed.

If the session addressed issues related to gender equality and/or women's empowerment, please provide a brief summary of the discussion:

There wasn't a specific issue related to gender equality and/or women's empowerment in the discussion.