Submission to the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

The Surveillance Industry and Human Rights

Mariana Canto[1]
Federal University of Pernambuco, Brazil
sobralcantomariana@gmail.com
@mariana__canto

February, 2019

Summary: This submission is a response to Part A1, A2 and B1 of the Special Rapporteur's call for submissions and is concerned with the use and importation of surveillance technologies and its regulation in Brazil.

Rio de Janeiro as a laboratory for foreign surveillance technologies

As the host country of events like Rio+20, the World Cup and the Olympics, Brazil and particularly Rio de Janeiro have become one of the main target markets for surveillance technologies. According to the local media, an investment of R$108 million was spent to build Rio's Centro Integrado de Comando e Controle (CICC) in 2013. Aiming the integration of several public databases, the Center acts as a base for monitoring the city, hosting workers from several agencies of the State, such as military, civil and highway police, fire and emergency departments and the traffic engineering company. However, gathering information on which kind of surveillance technologies were acquired with these figures is really difficult and mostly dependent on declarations from public agents or sellers of surveillance technologies to the press, leaks and, eventually, some access to information requests.

1 Mariana Canto holds a Law degree (L.L.B.) from the Federal University of Pernambuco, Brazil(UFPE) having studied part of her undergraduate program at the University of Hamburg, Germany. She is also part of the research and extension group DDIT(Discussing Digital Law, Internet and Technology) of the UFPE. Mariana is a former intern at the Internet Governance Forum (IGF) Secretariat at the United Nations Office at Geneva, Switzerland and former Fellow Undergraduate Researcher at the Brazilian National Council for Scientific and Technological Development (CNPq). Currently, she is an invited author of the Institute for Research on Internet and Society(IRIS).

According to news articles, the technology acquired by the different bodies of government and police include drones, facial recognition in airports and public transportation, mobile CICC station vehicles (equipped with movable cameras and audio capture), high-quality video surveillance balloons (with 13 cameras each), among others. An investigation by VICE News in 2016 discovered that a division of the Army (CCOMGEX, the Army Command for Communications and Electronic War) has a cell-site simulator (also known as an IMSI catcher) from US-headquartered Harris Corporation, for example.

In December 2018, it was announced in Rio de Janeiro, a partnership with the UK company Staff of Technology Solutions and the *Disque Denuncia* (a similar program to *Crime Stoppers* in other countries). According to the involved parties in the project, the so-called *Facewatch* system technology will enable the automatic identification of about 1,100 of Rio's most wanted criminals.

Zeca Borges, coordinator of the *Disque Denúncia*, states that for the service to work, it is necessary for the program to provide the database for the British company with images of the wanted ones. No information regarding the technology's privacy policy can be found on the company's website - only that it is GDPR compliant. In addition, access to more official information regarding the adoption, operation and effectiveness of the new measure is scarce in the media.

More recently, in 2019, Brazilian parliamentarians, most of whom are federal deputies of the PSL (President Jair Bolsonaro's party), traveled to China showing interest in the importation of the street camera system used for facial recognition of citizens. Initially, Chinese surveillance technology would be adopted in the state of Rio de Janeiro.

The PSL bench intends to present a bill in February to make mandatory the use of cameras for face recognition in public places, with the aim of identifying criminals and improving safety. The system consists of special cameras for the use of security organs, which would be installed in train and subway stations, airports, public high pedestrian streets and even at strategic points of communities dominated by the traffic and militias.

In a statement to Veja magazine, the elected deputy Carla Zambelli (PSL-SP), who is part of the group, said that this camera system could be implemented in 2019 without any cost for Brazil. Thus, according to Zambelli, China would not even be charging for technology and hardware components. In 2018, the social defense secretary of the city of Curitiba began a project that aims for the installation of hundreds of cameras throughout the city, capable of facial recognition of citizens and cars in real time. The project was budgeted at R$ 35 million, taking into account the budget of the similar project in Curitiba, one question remains: what will be the Chinese government's gain with this "donation"?

Via Quatro vs Idec: A significant victory for privacy

In April 2018, the agreement entered into between ADMobilize and ViaQuatro, the administrator of the yellow line of the São Paulo subway, enabled the use of a technology to collect data related to the facial expressions of public transport users. Almost four months later, on August 30, 2018, an action was filed by the Brazilian Institute of Consumer Protection (Idec) against this practice. After great public commotion in relation to the case, on September 14, 2018, Judge Adriana Cardoso ruled that the cameras had to be removed within 48 hours. According to the decision, "it is not clear the exact nature of the collection of the images and the way in which the data is processed by the defendant, which in fact should be disclosed to the passengers even more due to the public nature of the provided service." The judge also used the arguments provided by the Public Prosecutor's Office as a legal substantiation for the decision: stating that the usage of data collection of all users of the public transportation violates the right to information and the freedom of choice of approximately 600,000 consumers who use the service on a daily basis.

Recently, also at the yellow line in São Paulo, users of public transport reports the following message after an advertisement

Even though the verdict represents a significant victory for Brazilians' privacy, facial recognition technology has also been used by the State in public transport in other Brazilian capitals. In order to prevent fraud, cities are increasingly investing in mechanisms for verifying the identity of holders of special tickets that allow the service to be free of charge or to have reduced fares. However, in several cities there is still a lack of disclosure regarding the privacy policy related to the collection of users' data. A few months ago, the Observatory of Privacy and Surveillance criticized SPTrans of São Paulo for not being clear and public about its privacy policy for the *bilhete único* ticket. Likewise, Coding Rights produced a report on the RioCard ticket implemented by the city of Rio de Janeiro.

The existing legislation on the protection of civil liberties

The Federal Constitution of 1981 (CF) – The CF states in its Article 5, X, that:

"Everyone is equal before the law, without distinction of any kind, guaranteeing to Brazilians and foreigners residing in the country the inviolability of the right to life, liberty, equality, security and property, as follows: the intimacy, private life, honor and image of persons are inviolable, being assured the right to indemnity for the material or moral damage resulting from its violation."

The Civil Code of 2002 (CC) – In the same way, the CC of 2002 provides in its Article 21 the following provision: "the private life of the natural person is inviolable, and the judge, at the request

of the interested party, will take the necessary measures to prevent or terminate the act contrary to this rule."

The General Data Protection Law (LGPD) – Although Brazil has approved its General Data Protection Law in 2018, in force only in August 2020, the Article 4 of this legislation excludes "the processing of data for the purposes of public security" from its application. The law also allows the sharing of public data with companies as long as a supervisor authority exists.
According to experts such as Rafael Zanatta, as the law does not apply to data processing for public security purposes, it would be possible for authorities to argue that the data collection is for "identification of thieves and improvement of public safety." The Law states that the processing of data for public security purposes "shall be governed by specific legislation, which shall provide proportional and strictly necessary measures in order to serve the public interest" (article 4, III, § 1), however, the specific law does not exist until the present moment. According to Zanatta, the civic battle in Brazil at the present moment will be the collective definition of what are "proportional measures" and what is "public interest." The silver lining for some researchers and activists is the protection brought by general constitutional principles such as the presumption of innocence, and general principles of the LGPD itself, which fight against the abusive use of data collection. However, it is believed that a tremendous interpretative effort will be necessary in order to consolidate a jurisprudence where these principles will be applied in case of state surveillance, jurists such as Renato Leite from Data Privacy Brasil are already dedicating themselves to these issues.

Code of Consumer Protection of 1990 (CDC) – The Consumer Protection Code (Law 8.078 / 90), specifically in its article 43, establishes a series of rights and guarantees for the consumer in relation to their personal information present in "databases and registers". It is no coincidence that consumer protection continues to fill many of the gaps left by the lack of a specific regulatory framework related to personal data until the LGPD. In the ViaQuatro case for example the abusive conduct was noted and proven by the use of Articles such as 43 (access to collected personal data), 6 and 31, (informing consumers clearly about the prices of products and services offered). 6, V, 39, V, and 51, §1, I to III (manifestly excessive advantage) as legal basis by Idec.

The Habeas Data – Habeas Data, an institute that in Brazilian law takes the form of a constitutional action and was introduced by the Constitution of 1988. The Brazilian Habeas Data arose basically as an instrument for requesting personal information held by the public authority, in particular the bodies responsible for repression during the military regime.

Law on Access to Information (LAI) – The LAI was ennacted on November 18, 2011 to reaffirm the right of access to data produced or stored by organs and entities of the Union, State, Federal District and Municipalities. The law strengthens democratic concepts based on the value that citizens have the right to request and receive all information controlled by government bodies.

However, this year, access to information is being threatened after the Vice President Hamilton Mourão changed the rules of the game. The then-President-in-Office (President Jair Bolsonaro was in Davos at this moment) gave commissioned servers and managers of foundations, autarchies and public enterprises the right to impose ultra-secret secrecy on public data.

According to the NGO Article 19 in Brazil, the amendment to the decree that regulates LAI is detrimental to transparency by allowing more people to classify public documents as secrets and ultra-secrets, a factor that is likely to increase the volume of classified documents. The group sees an imminent decrease in transparency caused by the potential shortage of access and circulation of public information. This may lead to a violation of the right to information of the population as the society's ability to monitor public power and its public policies, understand political decisions, participate in a qualified manner, have social control will be reduced.

In practice, officials without permanent ties to the public administration (occupants of commissioned posts) are given a green light to classify official information with the utmost degree of secrecy: 25 years (for ultra-secret data) or 15 years (for secret data).

The decision generated strong demonstrations. More than a dozen agencies, including Abraji (Brazilian Association of Investigative Journalism) and Article 19 themselves opposed to the move of the Government.

It is certainly worrying that a decree that impacts on the right to information has been carried out without participatory processes, such as those that marked, for example, the elaboration of the Law on Access to Information in Brazil before it was approved in 2012. There was no dialogue with civil society or even with the other powers, including the legislative houses that approved the LAI. For the Article 19, the promulgation at the beginning of a new mandate brings an alert, indicating a tendency to reduce transparency and non-participation of the population in fundamental issues. It is important to continue to monitor the situation, always seeking to build paths, actions and partnerships for the prevalence of fundamental rights, such as access to public information.

Regulations related to the use of surveillance technology in Brazil

(i) Interception of communications Law

The Law 9.296/96, which regulates the use of interception of communications, brings some safeguards such as in its Article 5, which limits the period of surveillance to fifteen days. However,

as the period can be renewed for more fifteen days after renewable for equal an indispensable necessity of the evidence is proven, the legislation leaves a loophole and a possibility for abuse.
According to a study produced by Internet Lab study, a substantial increase was noted in relation to the number of judicial approval of requests for communications interception in recent years.

(ii) The Anticrime Bill

According to the Folha de São Paulo newspaper in 2015, the Brazilian Federal Police would be planning to install trojan horses in cellphones whose interception was already authorized by a judicial warrant. As this is a more invasive practice and with superior risks to citizen's privacy, this action would require not only specific legislation, but also a new judicial warrant that would allow such monitoring. Nevertheless, a quick analysis of the Brazilian normative framework indicates the absence of any legislation in the country that would authorize this kind of hacking.
Regarding the collection of data by police authorities for investigative purposes, as mentioned previously, there is in Brazil the Law No. 9.296 / 96, which regulates telephone or telematic interceptions, as well as the Law No. 12.850 / to crimes committed by criminal organizations. None of them, however, deals with the use of spy software for online monitoring and remote search of information in personal computer systems. According to researcher Laura Schertel, without a legislation authorizing the installation of the "spy software", setting limits and providing adequate safeguards, no legal basis exists for this action.
However, the new Anticrime Bill proposed by the new Ministry of Justice, Sergio Moro, includes a new Article in the Interception Law that would provide legal basis for government hacking - ie: infection of spyware devices by state authorities, allowing real-time monitoring and collection of what is stored in the device. It is necessary to remember that the NGO Access Now published a report identifying what are the main purposes of the state hacking and what are the techniques that serve such purposes. In general, the report indicates three situations used as justifications by the State: (i) control of speech and speeches on the Internet; (ii) infringe damages to certain targets of the State; and (iii) obtaining information for research and surveillance activities.