UNIVERSAL PERIODIC REVIEW – 4TH CYCLE

CONTRIBUTION TO ARGENTINA'S REVIEW

LACK OF OVERSIGHT ON THE USE OF TECHNOLOGIES FOR CRIME PREVENTION AND INVESTIGATION

1. The use of digital technologies for crime prevention and investigation may undermine human rights like freedom of expression and privacy, among others, if these technologies do not comply with the proper safeguards. In recent years, despite the commitments undertaken by the Argentine State,[1] problems of various kinds have been observed in the use of technological tools, such as use exceeding the limits set in regulations, lack of publicity and transparency in the hiring of private companies and agreements between state agencies, and the creation of vague, lax regulations without the necessary framework for discussion.

I. Facial recognition systems in the City of Buenos Aires and personal data protection

2. In April 2019, the Fugitive Facial Recognition System was put into operation in the City of Buenos Aires. Authorities stated this mechanism would be used "*solely for tasks required by the Attorney General's Office, the national, provincial and city judicial branches, and for the detection of persons sought exclusively under warrant and registered in the National Database of Fugitives and Captures (CONARC)*" (Art. 2 of the annex to Resolution 398/MJYSGC/19). The necessary information for said activity would be provided by national government authorities and sourced from CONARC records crossed with the personal data of those same people in the National Registry of Persons (RENAPER). It was expressly clarified that the latter set of data must correspond exclusively to people with a duly court-ordered warrant for their arrest (Art. 3).

3. On November 19, 2020, the City of Buenos Aires passed Law 6,339 amending Law 5,688 (on the city's Integrated Public Security System) and defined the facial recognition system as follows: "the Fugitive Facial Recognition System is intended for the identification and recognition of fugitives from justice based on the real-time analysis of video images." The law limited use of the system to tasks required by the national, provincial or city authorities, and to the detection of persons exclusively under arrest warrant registered in CONARC (Law 5,688, Art. 480 bis).

[1] See A/HRC/37/5 Voluntary promises and commitments "d) Argentina commits to continue promoting the necessary reforms to achieve improved levels of transparency, access to information, compilation of data and public statistics toward a better understanding of the human rights situation in the country."

4. In the context of legislative debates in Buenos Aires, civil society organizations underscored different concerns about the facial recognition mechanism. We pointed out that the mechanism could lead to arbitrary detentions and consequently impact the assumption of innocence, and the principle of equality and non-discrimination, given that facial recognition software has been repeatedly criticized for presenting bias in its margin of error based on color, ethnicity and gender. CELS (member of ICCSI) noted that facial recognition in video surveillance poses potential risks to rights such as privacy, freedom of expression and protest. It also added that this technology has been proven to have difficulties distinguishing persons with dark skin, leading to an endless number of false positives and disproportionately affecting groups who are already in situations of vulnerability.[2] The Ombudsman's Office for the City of Buenos Aires stressed the existing deficiencies in the CONARC database, sustaining that these "errors" could have been avoided if an impact study had been done before implementing the system to test the consistency of the database used. The Ombudsman petitioned the Supreme Court to remedy these errors. That impact study was not carried out and the CONARC database has not been updated. [3]

5. The United Nations Special Rapporteur on the Right to Privacy, Joseph Cannataci, commented on these issues during his visit to Argentina, and with regard to the system in the City of Buenos Aires, said, "I am aware of the need to detain persons suspected of having committed crime and bringing them to justice, but I do not see the proportionality of installing a technology with grave implications for privacy to search from a list of 46,000 people that currently includes minors and misdemeanors and that has not been updated or been tested for accuracy… The fact that facial recognition is being implemented without the necessary PIA (Privacy Impact Assessment), or a proper query and strong safeguards, is also reason for concern."[4]

6. Given these precedents and criticism of the facial recognition system, the social organizations disputed the use of the facial recognition system in justice matters. The Observatory on Digital Information Rights (ODIA) presented a collective *amparo*, and other organizations including ours joined that petition, currently in legal proceedings in the Buenos Aires contentious-administrative courts.

7. In the context of those proceedings, we learned that the Buenos Aires city government had accessed personal biometric data contained in the National Registry of Persons (RENAPER), which holds the data of more than 7.5 million people, meaning the city government exceeded the powers granted under the law to access said information. The city government was authorized to access the personal biometric data of the people in the CONARC database (i.e. wanted persons or fugitives from justice), also under the purview of the federal government, containing records on about 40,000 people.

---

[2]https://www.cels.org.ar/web/2020/10/la-legislatura-portena-debe-rechazar-el-uso-de-la-tecnologia-de-reconocimiento-facial-para-la-vigilancia-del-espacio-publico/

[3] https://srfp.odia.legal/cels.pdf

[4] Ibid, points 20 and 21.

8. The operation to access such a volume of personal biometric information was done through an agreement between the city government (Ministry of Justice and Security) and the National Registry of Persons (RENAPER). The agreement authorizes the government of the City of Buenos Aires to cross personal biometric data from the RENAPER database with the list of people with arrest warrants so as to locate them through security cameras equipped with facial recognition software. But, as we said, the list of wanted persons contains a much smaller number of just over 40,000 men and women, meaning the identification operation undertaken exceeded the authorized numbers by millions of individuals.

9. This situation, which city authorities have still not clarified or explained, highlights the lack of oversight on information exchanges between federal and provincial agencies of biometric data records in possession of the national State, based on personal identification information for the granting of national identity documents. Current regulations for personal data use set lax criteria for information transfers between state agencies (national and provincial) [5] At the same time, authorities use this lax basis to expand the possibilities for circulation of information among state agencies. The State has not developed mechanisms of oversight and monitoring in this arena on the use and utilization of information beyond the purposes for which it was collected, casting doubt on people's capacity to control how the State may use personal and/or sensitive information it collects on them.

10. Furthermore, facial recognition systems in Argentina are not limited to the City of Buenos Aires; they have also been implemented in various provinces and local municipal governments, without oversight on how they are used, the destination for the information compiled, or safeguards on the right to privacy.

II. The use of software in criminal investigations on which the National Ministry of Security has provided no information

11. In November 2020, together with a number of civil society organizations nucleated the Citizens' Initiative for Controls on Intelligence Systems (ICCSI)[6] submitted a request for information related to agreements made by the Ministry of Security in the framework of the Federal Plan to Prevent Technology-based and Cybercrimes and

[5] Art. 11 of Law 25,326 on personal data stipulates: "1. The personal data subject to treatment may only be granted for compliance with purposes directly related to the legitimate interest of the grantor and grantee and with the prior consent of the owner of said data, who must be informed of the purpose for which it is being granted and the identity of the grantee, or the elements that enable them to access it (…) 3. Consent is not required when:… b) in the circumstances provided under Article 5, paragraph. 2; **c) requested directly through State agencies insofar as the request is in compliance with their respective competencies;** 4. The grantee shall remain subject to the same legal obligations and regulations as the grantor and shall respond jointly and severally for the observance of said obligations and regulations to the control agent and the owner of the data in question.

[6] The Citizens for the Control of Intelligence Systems (ICCSI) initiative is a space for the monitoring, encouragement and promotion of effective functioning of oversight mechanisms on the intelligence-gathering system in our country, whose members are Centro de Estudios Legales y Sociales (CELS), Fundación Vía Libre, Instituto Latinoamericano de Seguridad y Democracia (ILSED) and Núcleo de Estudios de Gobierno y Seguridad of the Universidad Metropolitana para le Educación y el Trabajo (UMET).

the National Cybersecurity Strategy. We also requested a complete list of companies and representatives with whom the National Ministry of Security negotiates agreements to exchange information, training and cooperation in technology matters for the prevention of crime and, in particular, we inquired about the agreement for the use of software developed by the Cellebrite company, one of fifteen others announced in a Ministry press release.[7] On December 18, 2020, the Ministry responded that none of the agreements we inquired about had been signed.

12. On March 10, 2022, a social protest took place on the steps of Congress in opposition to the agreement with the IMF being debated in the legislature at that time. In the context of that protest, a group of people threw stones, causing damage to the office of Vice President Cristina Fernández de Kirchner and other congressional offices. In the context of judicial investigations to identify those responsible for the disturbances, news[8] became public about the use of facial recognition software by the Argentine Federal Police, which is under the purview of the National Ministry of Security. The web portals of the neither the Ministry of Security nor the Federal Police provide information about the use of tools of this type, but an article in the written press[9] revealed the specific use of the software "Luna Plataforma" for these purposes. On April 28 of this year, our collective of civil society organizations sent a request for information to the National Ministry of Security asking for public information related to the acquisition and use by said authorities of facial recognition software in criminal investigations. The ministry response does not provide basic information, such as the terms of agreement with the software provider company, protocols of usage, systems of oversight or confidentiality agreements. Moreover, the ministry also did not clearly respond as to the existence of other software programs by the security forces under its purview.

III. Surveillance on social media lacking any clear regulation

13. In April 2020, the National Ministry of Security reported that, in the context of oversight tasks to ensure compliance with restrictions of circulation imposed to prevent the spread of COVID-19, it was carrying cyber-patrol tasks. This action was protected in a ministry resolution passed in 2018 under the previous administration.[10] That resolution instructed the Cyber-crime areas of the federal forces to "take action" in a defined set of crimes through "investigative acts" to be carried out in online sites of public access. This regulation thus authorized

[7] Acciones para mayor eficiencia en la investigación criminal en el ámbito digital. Available at: https://www.argentina.gob.ar/noticias/acciones-para-mayor-eficiencia-en-la-investigacion-criminal-en-el-ambito-digital

[8] "Identificaron a ocho sospechosos por el ataque al despacho de Cristina Kirchner" Available at: https://www.pagina12.com.ar/407956-identificaron-a-ocho-sospechosos-por-el-ataque-al-despacho-d "Piedras en el Senado: detuvieron a un sospechoso por el ataque a la oficina de Cristina Kirchner" Disponible en: https://www.ambito.com/politica/cristina-fernandez-kirchner/piedras-el-senado-detuvieron-un-sospechoso-el-ataque-la-oficina-cristina-kirchner-n5393547

[9] "Exclusivo: los sospechosos y las pruebas de la investigación del ataque al Congreso por el acuerdo con el FMI" Available at: https://www.infobae.com/politica/2022/03/26/exclusivo-los-sospechosos-y-las-pruebas-de-la-investigacion-del-ataque-al-congreso-nacional-por-el-acuerdo-con-el-fmi/

[10] N° RESOL-2018-31-APN-SECSEG#MSG July 26, 2018

surveillance and/or intelligence to be conducted on open sources or social media sites without any precise regulatory framework around these actions. It did not clearly define the characteristics of these "investigative acts" or the scenarios in which they could be initiated. Furthermore, the regulation implied that such acts could be conducted without a warrant or judicial oversight, given that according to its Art. 2, once "the necessary means of evidence have been gathered," contact would be made with judicial officials. The brevity of definition of the crimes listed under this regulation seemed to be intended to hinder tasks of indiscriminate surveillance. However, the general and vague nature of this instrument generated grey areas by not clarifying what type of decision (or by whom) could initiate such actions by cyber-crime divisions.

14. In the face of criticism from different organizations, including CELS,[11] pointing to the measure's potential authorization of massive illegal surveillance and the need for these activities to be regulated, the Ministry of Security initiated a protocol project and convened a discussion table. Different proposals were presented there to improve the initial project and finally, in June 2020, a new resolution was approved and published in the Office Bulletin.[12] The new resolution sought to restrict the authorization of indiscriminate surveillance tasks, introducing the idea of "criminal indicators" and assigning the Security Secretariat (and not the police) with the task of defining them, although once again without specifying how they would arrive at such definition. Moreover, it set forth that the validity of this measure would remain in effect as long as the "public emergency" posed by the pandemic lasted, a fact that generates some uncertainty in regard to the regulation of these activities once the health crisis is over, and still pending discussion of a specific and permanent regulatory framework.

15. The new regulation established the creation of a Consulting Committee that, among other duties, is tasked with assessing the functioning of the protocol and proposing modifications or complementary provisions. The Cabinet of Advisors to the Ministry of Security can submit to the committee opinions and decisions, among other tasks, from civil society actors; and likewise can invite them to participate in meetings of the Consulting Committee. Since the creation of this regulation, the Ministry of Security has held two meetings in July and September of 2020 with the presence of civil society organizations. In November 2020, the organizations participating in the Consulting Committee meeting sent a proposal to the Ministry of Security on joint work, to which we have not received a response. On May 31, 2021, this same collective of organizations sent an information request to learn more about the application of this measure, to which the Ministry also did not respond.

Recommendations to the State:

---

[11] vigilancia en las redes sociales: pedimos información al ministerio de seguridad. https://www.cels.org.ar/web/2020/04/vigilancia-en-las-redes-sociales-pedimos-informacion-al-ministerio-de-seguridad-de-la-nacion/

[12] Ministry of Security Resolution 144/2020. Available at: http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=338229

1. The creation of directives and rules by the National Office of Personal Data and the Federal Agency on Access to Information relating to the use of personal biometric data for facial recognition systems in Argentina.

2. Promote regulations at the federal and provincial levels to require a Privacy Impact Assessment for the operation and supervision of facial recognition mechanisms.

3. Establish local and federal mechanisms for periodic checks of regulations authorizing the use of facial recognition in Argentina regarding its implementation with accountability across authorities and including monitoring by civil society.

4. Begin a discussion process on the need for a new law protecting personal and sensitive data, including biometric data as part of personal data and that must be protected by the State when forming part of public registries or banks of information.

5. Establish by law the legal framework in which security agencies can carry out criminal investigations through surveillance and intelligence tasks in open sources (OSINT) and particularly social media (SOCMINT).

6. Reinforce the commitment to the obligations of active transparency pursuant to Law 27,275 on access to information and the laws of each province and the City of Buenos Aires.

7. Establish policies on the obligation to publish the processes and terms of contracting, use and training in technologies used for crime prevention and criminal investigation.