



Buenos Aires, February 2019

Mr. David Kaye,

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

Ref.: Submissions on The Surveillance Industry and Human Rights

These comments were elaborated by the Center for Legal and Social Studies (Centro de Estudios Legales y Sociales - CELS). CELS is a non-governmental organization working to promote and protect human rights since 1979. It has a broad agenda that includes, among others, the defense of the rights to privacy and freedom of assembly and expression. This work is carried out today through strategic litigation both within Argentina and before international human rights bodies (Inter-American Human Rights Commission, Treaty Bodies, Special Rapporteurs, etc.) as well as through research, publications and other activities.

A.3. The lack of a known framework as these technologies advance

We have learned that the Argentine Ministry of Defense bought, through a deal with its Israeli counterpart, a surveillance software developed by a private company –Rafael Systems-, on the occasion of the G20 meeting that took place last year in Buenos Aires.

Although the agreement itself is not public, this specific purchase was published in Argentina's Official Gazette¹ and additional information was leaked in press articles². Nevertheless, what was exactly bought is still uncertain. What we have learned so far is that it works for CSIRT and CERT and, according to the media, this software can do massive and systematic analysis of the

¹ <https://www.boletinoficial.gob.ar/#!DetalleNormaBusquedaAvanzada/193298/20181005>

² See, for example, <https://somostelam.com/portal/el-gobierno-gasto-200-millones-en-tecnologia-que-puede-vigilar-redes-sociales/>

information it collects, either from open sources (OSINT) or non-open sources with previous consent.

This raises a number of issues in light of Argentine legislation: first, since this entails the massive and systematic analysis of information (not just its collection), it may clash with our National Constitution and the international covenants Argentina is party to, including the right to privacy, intimacy and freedom of both expression and movement, to the extent that the possibility of being subjected to constant surveillance and profile analysis may cause a “chilling effect” on participating in offline protests and manifestations.

In the second place, it is also problematic since Argentine legislation does not address this kind of intelligence. Although it is not forbidden, it is not specifically regulated either, meaning there is no clear framework indicating who can carry it out, under what rules and with what limits, who is in charge of overseeing it, etc. This could also represent a violation of the rights enumerated above, since it creates uncertainty for those willing to express themselves freely on their social networks. Moreover, as the law does not set any boundaries on what can be done with the information collected/profiles built based on this kind of intelligence, nothing prohibits the international exchange of this data, meaning the information could easily be triangulated.

The lack of oversight provided for in legislation and ineffective congressional and judicial control (as we will explain in the following section) make the use of this software even more dangerous.

At this point, it's important to mention that the advance of these technologies occurs in a global, regional and local context of securitization and weakening of political and judicial oversight mechanisms.

B.1. Emblematic cases of State use of surveillance technology against individuals or civil society organizations

There have been numerous allegations of online and offline surveillance carried out on local activists and potential political dissidents on the occasion of last year's G20 meeting, with the online spying possibly being done with this software. Although this has not been proven, there is a strong suspicion since it was bought for that purpose and there is no legal framework requiring that the use of this technology be informed or defining its boundaries or due oversight. Furthermore, as we will demonstrate, investigating what the government is doing on this matter is almost impossible

given the lack of Argentine legislation and poorly functioning institutions, especially in the judicial branch.

Therefore, although we cannot be certain due to the extremely opaque processes related to this matter, everything would indicate that this software has been used for surveillance.

What we are certain of is that surveillance through social media – with or without this kind of software – was carried out in another recent situation, in the case of the activists who were discredited from the 2017 WTO Ministerial Conference. This decision was made based on their social media posts, but we still do not know who made the decision and upon what specific information, as we will describe on the next section. This uncertainty is due to the impossibility of accessing public information connected to intelligence, security or defense in Argentina. In the next section, we explain the local context for trying to access this kind of information, highlighting two cases that we are currently litigating.

B.1.i. Litigation that we are carrying forward:

As mentioned before, in Argentina there are no known regulations regarding the export, import or use of surveillance technology. This does not mean such regulations do not exist, but we have no way of knowing: most of the information related to intelligence or defense falls into the “national security” exception in access to public information.

There have been many attempts to obtain this kind of information, sometimes leading to judicial cases. At CELS we are currently litigating several cases, fighting for our right to access public information on these issues. The following are our two main ongoing cases.

a. WTO disaccreditations

In one of them, we asked for information regarding disaccreditations from the 2017 WTO Ministerial Conference that took place in Buenos Aires. Sixty-five people from civil society organizations throughout the world received an email from the WTO saying that although their respective organizations had been accredited, security authorities in the host country (Argentina) had rejected their accreditation “for unspecified reasons”; two people on the list were ultimately deported³.

³ See CELS' press releases: <https://www.cels.org.ar/web/en/2017/12/omc-habeas-data/> and <https://www.cels.org.ar/web/en/2017/12/wto-meeting-in-argentina-rejected-accreditations-and-deportations/>

When controversy first broke out over the disaccreditations, the Foreign Affairs Ministry issued a press release explaining that the decision was made because these organizations or people “had made explicit calls via social media for violent demonstrations, expressing their intent to generate intimidation and chaos.” **Clearly, the government had been gathering intelligence, very possibly based on people’s organizational affiliation or political opinion – which is expressly prohibited under Argentine law.** That is why we requested that it specify the security parameters established for participating in an event of this kind and explain the relationship between that evaluation and prohibiting or hindering people’s entry to the country. We still do not know whether this surveillance was carried out using some kind of (private?) surveillance technology, through OSINT, or in other ways. **What we are certain of is that the disaccreditations were based on political opinions expressed on social media.**

In order to obtain more information about what happened, we filled administrative petitions. While some of these were *habeas data*, one was a public information request filed by CELS. In it, we asked the Foreign Affairs Ministry – which had been in charge of the organization and logistics unit of the Ministerial Conference – and the Federal Intelligence Agency (AFI) for information such as the criteria for prohibiting participation in the meeting and who was in charge of collecting the information and subsequently making the decision. Both agencies denied our request and shifted responsibility onto other state bodies, saying either that they had not ordered the disaccreditations or that all information regarding this issue was linked to national security/intelligence and was therefore absolutely secret. We filed a legal challenge to these responses and we are currently litigating the case before an appeals court, since the lower-court judge ruled that the agencies had provided enough information to comply with our request, hence validating the interpretation that all information connected to intelligence must remain secret.

b. ICCSI

Although not strictly related to freedom of expression, another case we are also currently litigating is connected to accessing the public information in possession of the Federal Intelligence Agency, which we are working on in conjunction with the ICCSI network⁴, as part of an INCLO joint project⁵. We solicited information regarding the regulation for the Agency’s reserved funds, quantitative data

⁴ The Citizen Initiative for the Oversight of Intelligence System (ICCSI) is a network of NGOs working for the democratization of the intelligence system in Argentina. See <http://www.iccsi.com.ar/>

⁵ The International Network of Civil Liberties Organizations’ (INCLO) international intelligence sharing project. See <https://www.inclo.net/projects/international-intelligence-sharing-project/>

on wiretappings and whether international intelligence-sharing agreements have been forged with other countries' intelligence bodies. Similar to the case described above, this case began as a FOIA request, the denial of which led to proceedings in court. The lower-court judge showed complete deference to the executive branch, so we appealed and we are currently awaiting the appellate court ruling. This case shows once again: a) the impossibility of accessing information regarding the intelligence system in both administrative and judicial processes; b) the lack of regulatory frameworks for these matters; and c) the inexistence of suitable mechanisms to protect against this kind of surveillance.

CONCLUSION

Argentina's intelligence system continues to operate with little transparency and questionable legality. The ban on collecting information on people based on their political or ideological views has been flouted again and again, in different cases that have come to light. The use of ideological and political criteria to gather intelligence is against the law and any action taken on the basis of this information or analysis is illegitimate. Furthermore, there is no known regulatory framework nor effective oversight mechanisms in place.

The process for accessing public information when state security may be involved is highly difficult and opaque. Both the administrative and judicial procedures are inefficient, and there is no intention of controlling what information is being produced and gathered by intelligence bodies, who is being spied on and under what criteria, to determine whether those activities are legal. The argument of "state security" serves as a generic answer to block any attempt to access information possessed by intelligence bodies, even when general and quantitative questions are being asked.

Moreover, the Bicameral Intelligence Committee of Congress – created under the National Intelligence Law and which has the responsibility of supervising the Federal Intelligence Agency's (AFI) procedures for obtaining and gathering intelligence – has not been very active and has never referred to the legality of intelligence bodies' activities in any of its reports. This is why we continue to insist on judicial review, which has shown itself to be absolutely deficient thus far.

In particular, this creates a very uncertain scenario for all activists: surveillance can be carried out at any time through social media or by other means with disproportionate affectations to human rights, and no regulatory framework or effective administrative/judicial review.

This is, of course, a very discouraging scenario for freedom of expression, with no regulations on the use of surveillance mechanisms and absolutely no effective oversight (by either the executive, judicial or legislative branches of government). This lack of clear frameworks and proper checks evidently contradicts the obligations the state assumed under Article 19 of the International Covenant on Civil and Political Rights (ICCPR), since there is no way to ensure the freedom of expression of those willing to protest or demonstrate publicly – online and offline.

So far, we have witnessed worrisome judicial deference to the executive branch of government. Courts are not resolving the cases in accordance with the ICCPR or the standards of international human rights law on this matter. In this regard, a report from your office setting clear and well-defined standards would be very valuable for Argentine courts' interpretation of our National Constitution and the ICCPR.