CONVERSATION

"WE NEED GREATER TRANSPARENCY AND DEBATE ON THE USE OF SURVEILLANCE TECHNOLOGY"

• *Interview with Jamila Venturini and Michel Roberto de Souza - Derechos Digitales* •

By *Sur Journal*

Derechos Digitales[1] *is a Latin American organisation, committed to the defence and promotion of human rights in the digital environment. It works in three main areas: freedom of expression; privacy and copyright and access to knowledge.*

For this issue, the Sur Journal *had the opportunity to talk to Jamila Venturini, co-executive director and Michel Roberto de Souza, director of public policy at the organisation. Our main interest, as well as finding out about the results of the recently published research by Derechos Digitales on cases of facial recognition in Latin America,*[2] *was to hear the reasons for the accelerated growth in the use of surveillance technology and facial recognition and the consequent risks for human rights, based on information from an organisation specialised in this matter and in this region.*

Issues covered in this conversation include, for example: local and international legislation; economic and political relationships between manufacturers, providers and buyers; details about the application of this technology in different contexts across the continent; the impact of the Covid-19 pandemic on the legitimisation of greater surveillance in the control of public and private space; increased racial and migratory discrimination as well as the principal challenges in the region in terms of guaranteeing the right to privacy, autonomy and access to citizens´ information.

Sur Journal • In recent years we have seen a panorama of advancing surveillance technology in countries of the Global South. What analysis do you make of this scenario?

Jamila Venturini • Our concerns with surveillance and privacy in the digital arena are closely linked to the observation that this technology is added to a history of human rights abuse and the criminalisation of groups that oppose established power structures in Latin America. It is possible that this technology will not only facilitate intrusions into private communication but also allow access to information that has not previously been available to the police and authoritarian governments. One example is metadata, in other words the ´tracks´ we leave with every interaction on digital devices. These include geolocation, internet connection time and duration and access to certain pages or platforms etc. In addition, metadata reveals individual intimate and sensitive habits about where and how we live, our contact networks, our interests and thoughts, when we sleep... Unfortunately, there have been a number of examples of abuse in relation to the use of this type of information, by both the public sector and businesses.

As well as a series of legislative developments that seek to ease government access to private information, harvested by companies offering a wide variety of types of technology, we have observed a growing interest in the region in purchasing surveillance systems. In addition to recording what happens in public and semi-public spaces, they seek to extract even more information on human behaviour and force access to devices, as is the case of biometric systems, like facial recognition, and malicious software, also known as malware.

This interest stems, to a great extent, from the perception that technology will help to solve social problems. In the arena of public security, this rhetoric is used to defend both the purchase of a wide-variety of technology and reforms to norms that allow its use. It is worth remembering that Latin America is a great consumer of foreign technology and is not known for its local production. In this sense there is considerable concern over Latin American countries becoming a privileged market for manufacturers and distributors of surveillance technology, especially when controls tighten in other regions of the world.

Sur • How has the debate of surveillance been panning out in Brazil?

JV • In Brazil we know how much this type of technology is gaining ground in small towns, in a number of public spaces, quickly and with very little transparency. The way in which citizens find out this is happening is when it gets into the press or when a public purchase of cameras is identified, for example through a bidding process. This is always too late and the purchase or adoption of this technology is already well underway. This is happening in a country that has a history of authoritarianism and abuses. Legislative progress and existing norms cannot necessarily provide the guarantees needed for this type of technology to be used in a way that is aligned with adherence to human rights as committed to by Brazil. This is not a simple debate and very specific criteria are needed about how and to what extent surveillance technology will be used.

Michel Roberto de Souza • It is also pertinent to mention the press and journalists who have a history of censorship and persecution in the region. We have seen many examples in which state patrols start at the digital level, what we call *ciberpatrullaje*,[3] collecting information from a variety of sources, including open ones, on the internet, the motive and purpose of which are usually questionable as they are used to stigmatise journalists, activists and human rights defenders who hold opinions that differ from those of the incumbent government. Social media searches are used, with telephone access and spyware, such as the recent case of Pegasus. It is clear that the violation of rights starts in the digital [environment], but then moves to the physical one. Technology is increasing the potential for persecution. This is why the matter of the tracks left on the internet and the need for end to end encryption are important, as are other human rights protection issues.

In the case of facial recognition in public places this is so much more important. With this technology it is possible to find out who a person is, what the nature of their movements are and who they are talking to. A variety of information, much of which, although collected in public spaces is extremely sensitive, is captured on cameras that are often hidden. Not to mention the serious problems related to discrimination and false identification, as well as the possibility of crossing-referencing data with a variety of other databases.

We are seeing a trend of states wanting to have more data about their citizens, across the whole of Latin America. Huge databases are being set up and facial recognition data is taken and cross-referenced with data from the streets, metros and daily life, generating an enormous quantity of information about everyone. Everyone being journalists, human rights activists, people who protest on the streets, women, transsexual people, children and teenagers, migrants... There are many risks involved. Peaceful assembly and the very right to protest could be under threat. It is possible to know who is protesting because it is very easy to find out and to cross-reference. There are also threats to freedom of movement and circulation, to the presumption of innocence, the right to be considered innocent until proven guilty, and not to be investigated without the correct legal procedures. This use of technology also raises very serious questions about privacy, intimacy and data protection.

Sur • How does this exposure of data and information occur and how is it related to discriminatory practices?

MRS • The data collected by a facial recognition system is sensitive biometric data which is then stored somewhere, but we need to ask how it is stored, who has access to it and which data is cross-referenced. Which databases can be used for this? Are there any security risks? We recently saw an organisation in Mexico, R3D, that reported a case of seriously vulnerable security cameras which could easily be hacked.[4] So we have a state with hyper-surveillance, but the surveillance itself has huge security flaws that expose citizens even more, not to mention questions over the legality of hyper-surveillance.

There are grave risks to freedom of expression and censorship, with a tangible reticence to debate publicly and people censoring themselves because they know they are being surveilled. This is evident among journalists and human rights defenders. For example, it is difficult to carry out investigations and maintain contact with sources because this will all take place in an environment of surveillance. In addition, there are issues involving discrimination which are very clearly happening around the world mainly due to flaws in this type of technology, particularly in processing people who are not white men. In other words, in processing women, people with dark skin, black people and also children. There have been a variety of problems related to discrimination, such as arbitrary imprisonments and other illegal acts. There are migration issues too as we know that immigrants are being increasingly surveilled in a number of ways and that states are using a wide range of technology for surveillance.

We have been talking a lot about how technology is being used to move migrants on, including some serious cases of hacking mobile phones and social media, among other abuses. These cases are not only occurring at the borders, but also involve facial recognition in towns to find out where migrants are, who they are talking to and whether they are in the country legally or not.

As such, there are high risks related to technology in a broad sense, but also to facial recognition in a stricter one. The use of tools with so-called artificial intelligence are being widely debated in terms of the use of technology and of technological solutionism, the idea that AI can be used and is good for everything, from the simplest to the most complicated tasks. Facial recognition employs artificial intelligence which is how things connect up.

Sur • With regards to Latin America, what are the identifiable contradictions in terms of valuing technological tools for surveillance and the curtailment of individual and collective freedom, for example?

JV • We see many contradictions in our region and widely varying applications of surveillance technology. The first point to stress is that surveillance still exists in its more archaic format, with agents pursuing members of the political opposition in some countries, reaching highly sophisticated levels like the installation of antennas to pick up communications, facial recognition cameras and the installation of malware. This type of strategy has been used against journalists, social movements and human rights defenders with the aim of silencing, criminalising and persecuting these groups of people.

The second point is related to the question, almost a cliché now, "who surveils the surveillant? We are seeing a growing trend in the harvesting of citizens´ data by states, as well as attempts to place burgeoning restrictions on access to public information as well as constraints on public transparency initiatives. This became evident during the pandemic. While governments announced their strategies on the basis of sensitive data harvested to inform on people's movements and health conditions, they also sought to curb public access to information on state activities. This was especially apparent in Brazil and

is totally unacceptable. Any state activity that could result in constraints on the exercise of fundamental rights must be accompanied by strict transparency measures, among others, as highlighted by a number of international human rights bodies and authorities.

Finally, it is important to acknowledge that surveillance is also taking place unequally across society and is directed differently towards different groups of people. When there is a proposal to install facial recognition cameras on the metro, for example, or on any form of public transport, this will affect the people who use public transport and not those who use other options. This is not a new discussion, but it is always important to emphasise it. Surveillance has affected, and continues to affect, populations that have been historically marginalised and, with the help of new technology, like artificial intelligence, it is reinforcing inequalities. In the region we are already seeing how certain types of technology are used to legitimise state intervention in highly vulnerable areas. In Argentina and Chile, for example, a system is being pursued that will 'foresee' situations like teenage pregnancy, truancy and others, based on the harvesting and cross-referencing of a series of personal data. In other countries, proposals for the use of predictive policing, which are the subject of hot debate at the international level, are being tested.

Sur • What is your perception regarding regulation and its capacity to curb the perverse use of surveillance software?

JV • Scenarios are varied and depend on the country and the type of technology in question. It is one thing to talk about telephone tapping and telematic tracking,[5] which have to follow a number of very strict criteria regarding procedures, so they are done in the least intrusive way possible and only in very specific limited cases. In this sense there is a broader consensus and established rules exist, both of which could be extrapolated to other practices, like cyber patrolling, breaking cryptography, etc. It is another thing to talk about video surveillance and facial recognition, which are forms of mass surveillance and there are many questions about the extent to which they are compatible with existing human rights benchmarks, fundamental to criteria of legality, necessity and proportionality.[6]

There is a wide international debate on the legitimacy of buying and selling surveillance technology and the need for a moratorium or prohibition of this type of business, given both the institutional fragility of the countries that are buying it and the failure of the companies producing it to guarantee that it does not generate risks to human rights. The responsibility for guaranteeing that the technology they produce is safe; does not generate excessive risks to human rights; and is not being provided to authoritarian governments lies with these companies.

However, given the indiscriminate advances made by this type of technology in the region and the lack of specific regulation, there is a need to think about the rules that are required to mitigate risks and about inspections and monitoring that will have to be guaranteed, with democratic participation.

MRS • How, where and with which regulatory tools? These questions have not yet been answered, however we do have some hints. In the last few months, Michelle Bachelet, the UN High Commissioner for Human Rights, published a very precise and important report, pinpointing the high risks to society of using technology and artificial intelligence and requested a moratorium on the use of this type of technology until states have managed to comply with a series of human rights requirements,[7] taking into account the design life of this technology from the beginning to the end. This monitoring is vital.

Sur • What main challenges, in terms of human rights, privacy and security does facial recognition as a strategy of surveillance and control, present to Latin American human rights organisations?

MRS • We often find it difficult to understand how this type of technology works and how it is being applied, as we are talking about extremely opaque conditions. We do not know who makes it or what the law that regulates it is. In addition, this type of technology has no specific purpose in contexts where there is no social participation. This seems like a purely administrative day-to-day issue and as such it would not be necessary to listen to the general public or the people who are affected. In fact, it may appear that there is no need for debate. But it is precisely the opposite: we need greater transparency and debate on the use of surveillance technology given the huge negative impact on peoples' lives. For example, because of the murky nature of the issue of facial recognition, Derechos Digitales has launched a site[8] and has recently carried out research in collaboration with the Al Sur consortium, a collection of 11 Latin American organisations. We pinpointed around 40 initiatives for the use of facial recognition in the region. In Brazil, we found 4 or 5 initiatives, but we know there are many more.[9] Therefore, the very existence of this type of surveillance technology is an enormous challenge.

More recent research by other organisations has shown that the challenges in adopting technology without due care to respecting human rights are enormous. In Brazil, organisations are looking into how facial recognition interferes with the rights of trans people, for example. Coding Rights carried out this research and these are extremely important studies because they provide a different perspective on the problems and negative impacts of using this type of technology.[10]

It is important to question and to provide more transparency. But when we pose these questions to public authorities, they simply do not have the answers. They just have an idea that they are going to find solutions and solve some or a number of problems in one go, that this will be good for public security and will reduce crime rates, but they do not know how this technology will actually solve the problem. On international forums, the UN itself has recently reviewed the resolution on privacy in the digital era, presenting the risks of the use of biometric technologies and artificial intelligence. Likewise, UNESCO has adopted an agreement on artificial intelligence in an attempt to raise some issues, as well as emphasising the need for an ethical impact assessment.[11]

Sur • How does raising awareness function among the people who are directly affected and how have strategies and dialogue been approached by organised civil society itself?

JV • As I mentioned earlier, civil society generally finds out about this type of technology when it is already too late, in other words once the purchase is already underway. So, an alternative route is judicial questioning with the aim of preventing implementation and obtaining information.

For example, we saw a number of cases, in our survey, of very precarious administrative management. So, the fact that we have this limitation in how the discussion is presented within the benchmark of human rights, slightly reflects the difficulties we have mentioned. And this is not necessarily exclusively surveillance technology or facial recognition systems, as we are in a period of many different setbacks to the human rights agenda in the region. Indeed, there is still a lot to be done in terms of how we understand the criteria of legality, necessity and proportionality when dealing with facial recognition systems and surveillance technology.

This is a challenge, but at the same time there is a need for a big effort to raise awareness, now, as this technology progresses so intensely, among people working on public management, handling contracting, making decisions and formulating public policy. This is also needed with judicial authorities, in order to bring about effective controls on how the technology is implemented. Because we are talking about something that is escaping legislative debate.

The debate is only happening once technology has already been processed at the administrative level, often after judicial questioning. But, civil society is also important in understanding these trends and trying to chart what is happening, where it is being implemented, which companies are trying to push it through, because then other strategies and other responses can be sought, in other regions too, for example, in the companies´ countries of origin and on other types of forum. There are still challenges and the urgent concern is how we can get involved in this debate as human rights organisations, how we respond to these initiatives and what types of arguments emerge... There is a lot of unawareness and sadly we have even observed attempts to use and support this type of technology by civil society organisations. We must continue to work together towards a common understanding and then the next step will be with those responsible for formulating public policies. Certainly, winning over public opinion is one objective, but the challenge is far greater than this in terms of how we mobilise socially to benefit human rights in the broader sense.

MRS • The debate has moved slightly out of the arena of those who work with technology. Concerns have been reaching civil society in a broad form as well as those who deal with these themes on a daily basis. For example, those who are dealing with themes concerning racism, the rights of children and adolescents, migration, freedom of press and other themes. Civil society has been showing considerable interest in the matter of facial recognition in particular, but also in the use of other surveillance technology. There is, however, a lack of perception

that this is in fact a human rights risk and problem. We are in the initial stages of identifying this as a problem in different areas of civil society activities in order to go on to influence and to try to carry out strategic litigation with the participation of a variety of players.

Social participation must be fostered in a wide range of different areas. As a lawyer working in the area of technology, human rights and litigation, I see the issue of technology in a particular way. But, when a journalist or an association of journalists are handling a technology issue, they will see it in a different way. There is an immense richness in this exchange of understanding. In some countries the perception of the use of this type of technology as a problem is evident, like in Mexico, with all the attacks that are happening there and the importance of verifying how technology is being employed to violate rights. This reveals and creates possibilities for civil society to come out in defence and to show much-needed resistance.

Sur • From the research you are developing, how do you see the relationship between the countries that are producing this type of technology and the countries of Latin America and how does lobbying occur, principally on the issue of public security which is perhaps one of the areas in which it is being employed most widely?

JV • What we have done is to chart it. We identified, for example, that there are international companies working in the region in different ways. For many years – according to our research, since the 1990s – a number of countries have had agreements with these companies. In addition, there are also usually local dealers working for these international systems. Another factor we observed, which had already been a hypothesis of ours, is the involvement of Chinese companies. They work differently. They provide services and at the same time, the Chinese state offers funding for hiring this type of service. It is almost as though the service is being donated. There are also cases in which there is either no economic cost or reduced costs.

So, when we think about facial recognition there are a number of providers involved: people involved in infrastructure; telecommunications etc, and there are national and international companies. It is interesting to note how international businesses are operating in the region, with support and contracts worth millions. In the most evident case, we identified Chinese companies, forbidden to operate in some countries under serious suspicions of involvement or use of their systems in the context of human rights violations. We particularly found these cases in Mexico. Moreover, the fact that it is such a complex supply chain makes it even more difficult to identify all the agents and each of their roles.

When we consider lobbying and how companies work here, one issue is that it seems there is a difference between how they operate in their countries of origin and how they operate in the region and not only in terms of facial recognition. Last year, a number of companies stated that they would not sell their facial recognition technology to police forces. But when we investigated this statement further we found it is sometimes applied only at the

national level. For example, in the United States, on the backdrop of the Black Lives Matter movement, a number of companies, like Amazon, IBM, Microsoft among others, stated they would not sell their systems, but it remained unclear whether they would be sold globally, whether they would only not sell locally and to whom they would not be sold and for how long... These are some of the limitations of this type of proactive measure. So, one big challenge is understanding how these companies see themselves on a global scale. Another challenge, when dealing with surveillance companies, touches on the extent to which there are mechanisms for demanding accountability for these companies and to what extent this has been effective. We are able to have some ideas but without much evidence regarding lobbying. We know that there are often direct relationships that happen at the administrative level between salespeople and buyers.

Derechos Digitales is a member of a global multi-stakeholder organisation called Global Network Initiative (GNI), which brings together companies, civil society organisations and academics who work on resisting obligations imposed by specific states that carry out abuses related to privacy and freedom of expression. These issues vary greatly depending on what is being analysed, which sector of the company and definitely which country. As there is not a particularly robust legislative discourse concerning facial recognition, lobbying comes from other quarters.

MRS • Some companies have said they will not use this type of technology and that they have self-imposed, shall we say, a moratorium regarding facial recognition, but, they also want regulations. The discourse is that regulations are necessary in some format in order to avoid greater human rights risks. The truth is that the public security market is big, global and worth billions, but there is also the market of facial recognition and surveillance in general. We know that there are many companies carrying out legislative lobbying, but it is difficult to find out who they actually are, what their interests are and the arguments they are levying. And it is even more difficult at the local level, for example, in schools and projects for smart cities. Finding out who is lobbying is difficult. We have some clues, some suppositions...

Sur • What are the future prospects for this debate?

JV • Some years ago, we imagined that by now we would have a positive constructive agenda regarding the use of technology. The agenda exists and persists. It is still at the centre of our concerns, but we are experiencing a period of many challenges and many setbacks that could be made worse by surveillance technology. This means we have to mobilise more and more to resist it and to try to raise awareness about the risks it presents. We sometimes feel rather technophobic, the complete opposite of technological solutionism, but most of the efforts that need to be made now, in that most of this technology has a great appeal in society, in different sectors and states etc, is to debunk some of the assumptions that underpin the use of this technology. I believe a critical vision is fundamental in establishing the bases for dialogue about what we want from the use of

the technology, the norms we want, that will sometimes be needed to regulate the use and that will need to be specific, also in the area of investigations. As I said in the beginning, there are times when we need to turn to certain technology and certain information, but this must be very limited. Sadly, we are seeing a trend that is the opposite to this, and an attempt to allow the maximum possible use and access.

We are experiencing a time of defending our most fundamental rights, knowing that when we speak of privacy we mean a right that is instrumental for a number of other rights. It is important to understand that this is not simply an individual right, my right to not be bothered in my communications, it is basically a question of my being able to interact and develop my autonomy and express myself freely. And as such also allow society as a whole to have access to a series of other information and visions of the future and of reality. All things are highly interconnected. We are talking about things that also affect the extent to which our democracy can flourish, or not. These are not just individual issues. It is essential to bring this back into the conversation.

• • •

Interview conducted by the Sur Journal *team in November 2021.*
Original in Portuguese. Translated by Jane do Carmo.

"This journal is published under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License"