CELE
Centro de Estudios en Libertad de Expresión

Research Article

57b

Open Source Intelligence (OSINT) and Human Rights in Latin America: A Comparative Study in Argentina, Brazil, Colombia, Mexico, and Uruguay

Nicolás Zara

September 2023

Nicolas Zara, "Open Source Intelligence (OSINT) and Human Rights in Latin America: A Comparative Study in Argentina, Brazil, Colombia, Mexico, and Uruguay", Artículo de investigación No. 57b (ENG),
Centro de Estudios en Libertad de Expresión (CELE), Buenos Aires (2023)

UP
Universidad de Palermo

Facultad de Derecho

Centro de Estudios en Libertad de Expresión

Open Source Intelligence (OSINT) and Human Rights in Latin America: A Comparative Study in Argentina, Brazil, Colombia, Mexico, and Uruguay

Nicolás Zara[1]

Researcher

nicolaszara.cele@gmail.com

September 2023

Abstract

The use of OSINT by the state for surveillance purposes presents specific challenges regarding human rights. These tools can lead to violations of fundamental rights and are often employed outside the boundaries of legality. As this study will show, their use is generally unregulated, and where regulations do exist, they are inadequate. Under broad and vague definitions, intelligence and security authorities monitor open sources of information on the internet, such as social networks, blogs, magazines, and newspapers. In some cases, the collected information is organized, systematized, and incorporated into intelligence reports, which may include the profiling of citizens. This report aims to provide an empirical approach and a comparative analysis of the use of OSINT by states in the Latin American region for surveillance purposes. It is a field study that seeks to assess the scale of these techniques' use, identify the actors involved, and, where measurable, evaluate their impact and effectiveness. This research was conducted by a consortium of organizations, including Article 19 Brazil and South America, Article 19 Mexico and Central America, the Center for Studies on Freedom of Expression and Access to Information (CELE), Datysoc, and Fundación Karisma. The coordination was led by CELE, which proposed an analytical-qualitative framework as the study methodology.

Keywords: open source intelligence, surveillance, OSINT, privacy law, freedom of expression

---

[1] Researcher at the Center for Studies on Freedom of Expression and Access to Information (CELE-UP). Lawyer graduated from Universidad de Buenos Aires with a specialization in public law. He holds an LL.M. (Master of Laws) from Tulane University and is pursuing a Master's in Constitutional Law and Human Rights at Universidad de Palermo. Constitutional Law Professor at the Universidad de Buenos Aires. This work stems from research initiated in 2022 at CELE, building upon a preparatory study on the topic authored by Eduardo Bertoni. The author thanks Morena Schatzky, who previously led the research and drafted an initial version of this work, as well as Agustina Del Campo, Ramiro Álvarez Ugarte, Paulo Lara, Catalina Moreno, Juan Pablo Parra, Martha Tudón, and Patricia Díaz for their invaluable contributions and comments.

I. Introduction

Among the many changes that the internet has brought to contemporary societies, one of the most problematic is the increase in the State's surveillance capacity over its citizens.[2] Today, the amount of information available online about individuals is larger than ever. As that volume of information grows, the mechanisms for collecting, processing, and storing it become increasingly effective.

The information we leave behind through our online interactions is routinely collected and used by companies to provide advertising services to third parties, who in turn market their products or services to us. Additionally, there are other traces we leave behind that anyone can collect and process to learn a great deal about us—even states, for purposes that may range from relatively benign to highly problematic.

Open Source Intelligence (hereinafter OSINT) is part of a set of terms that refer to intelligence techniques such as COMINT,[3] SIGINT,[4] HUMINT,[5] GEOINT,[6] etc. OSINT can be understood as the collection and analysis of information gathered from open (and publicly available) sources to produce actionable intelligence. It is only when this information is given a specific purpose or use and linked to a concrete action that it becomes actual intelligence.[7]

---

[2] United Nations (UN), Human Rights Council, "El derecho a la privacidad en la era digital," Report of the United Nations High Commissioner for Human Rights, A/HRC/27/37, June 30, 2014, § 2.

[3] Communications Intelligence (COMINT) refers to information collected from individuals' communications, including phone conversations, text messages, and other online interactions. For further information, see Tech Target, "COMINT (Communications Intelligence)," retrieved from: https://www.techtarget.com/whatis/definition/COMINT-communications-intelligence, last access: August 9, 2023.

[4] Signal Intelligence (SIGINT) involves gathering information by intercepting a wide range of signals (e.g., radar or other systems). For more details, see Everything RF, "What is SIGINT?" 2022, retrieved from: https://www.everythingrf.com/community/what-is-sigint, last access: August 9, 2023.

[5] Human Intelligence (HUMINT) is the term used for collecting information from human sources. For further information on Odin-OSINT and Cyberintelligence, see "Qué es la HUMINT, ejemplos, técnicas y su relación con OSINT," 2022, retrieved from: https://odint.net/humint-osint, last access: August 9, 2023.

[6] Geospatial Intelligence (GEOINT) involves obtaining information about locations and geographic areas—typically through maps, on-site observations, imagery, or geographic information systems. For more on this, "Qué es la GEOINT y para qué se usa la inteligencia geoespacial," Odin - OSINT y Ciberinteligencia, 2022, retrieved from: https://odint.net/geoint, last access: August 9, 2023.

[7] ADC, "Seguidores que no vemos. Una primera aproximación al uso estatal del Open-Source Intelligence (OSINT) y Social Media Intelligence (SOCMINT)," 2018, retrieved from: https://adc.org.ar/wp-content/uploads/2019/06/045-seguidores-que-no-vemos-10-2018.pdf, last access: August 9, 2023.

The current global landscape shows a growing trend in the development, acquisition, and use of mass surveillance technologies by states.[8] The regional context is similar.[9] This trend intensified with the increased use of such technologies following the onset of the COVID-19 pandemic.[10] Moreover, states are often reluctant to provide information about their use of surveillance technologies.[11] Cases of illegal state espionage have multiplied across the region, typically targeting political dissidents, human rights defenders, protesters, union members, and journalists.[12]

---

[8] UN, (n. 2), § 2.

[9] Centro por la Justicia y el Derecho Internacional (CEJIL) et. al., "Organizaciones advierten riesgos de tecnologías de vigilancia en audiencia ante la CIDH," 2021, retrieved from: https://cejil.org/comunicado-de-prensa/organizaciones-civiles-advierten-riesgos-a-los-ddhh-sobre-tecnologias-con-capacidades-de-vigilancia-en-audiencia-ante-la-cidh, last access: August 9, 2023.

[10] In Colombia, the Security Forces have reportedly been conducting "cyber patrolling" since at least 2015, based on Article 15 of Resolution No. 5,389, dated December 31, 2015, issued by the National Police. These activities are carried out without being subject to regulations that establish standards for their operation. For example, see the Colombian government's response to the public information request made by the Fundación para la Libertad de Prensa (FLIP) regarding the use of "cyber patrolling" for detecting "fake news" (Ministry of National Defense, National Police, Criminal Investigation Directorate and Interpol, No. GS-2021, DIJIN-CECIP-1.10, June 30, 2021, retrieved from: https://drive.google.com/file/d/1Z7AKesIM_LY5Jde-8tH2mQnDbyNZCc2a-/last access: August 9, 2023). In Argentina, Resolutions No. 31/2018 and No. 144/2020, now repealed, authorized "cyber patrolling."

[11] Regarding the case of Colombia, see Fundación Karisma, "La punta del iceberg. Los problemas de transparencia del OSINT en Colombia," 2023, retrieved from: https://web.karisma.org.co/la-punta-del-iceberg-los-problemas-de-transparencia-del-osint-en-colombia, last access: August 9, 2023.

[12] See, for example, the Inter-American Commission on Human Rights (IACHR), Office of the Special Rapporteur for Freedom of Expression (RFOE) and the Office of the United Nations High Commissioner for Human Rights (OHCHR), "La CIDH, RELE y OACNUDH expresan preocupación ante los hallazgos sobre uso del software Pegasus para espiar a periodistas y organizaciones de la sociedad civil en El Salvador," Press Release No. 22/2022, January 31, 2022. Scott-Railton, John et al., "Project Torogoz. Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware," Munkschool of Global Affairs & Public Policy, University of Toronto & The Citizen Lab, 2022, retrieved from https://tspace.library.utoronto.ca/bitstream/1807/123609/1/Report%23148--project-torogoz.pdf, last access: August 9, 2023. Article 19 Mexico, Red en Defensa de los Derechos Digitales (R3D) and Social TIC, "Gobierno espía: vigilancia sistemática a periodistas y defensores de derechos humanos en México," 2017, retrieved from: https://r3d.mx/wp-content/uploads/GOBIERNO-ESPIA-2017.pdf, last access: August 9, 2023. FLIP, "Inteligencia Militar incrementa su capacidad para vigilar a periodistas y ciudadanía con tecnología de fuentes abiertas," 2023, retrieved from: https://www.flip.org.co/index.php/es/publicaciones/informes/item/3007-inteligencia-militar-incrementa-su-capacidad-para-vigilar-a-periodistas-y-ciudadania-con-tecnologia-de-fuentes-abiertas, last access: August 9, 2023. See also the case of Colombia, which was listed among the clients of spyware used against journalists and political leaders in 2021. Dvilyanski, Mike, Agranovich, David and Gleicher, Nathaniel, "Threat Report on the Surveillance-for-Hire Industry," Meta, 2021, p. 10, retrieved from: https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf, last access: August 9, 2023.

In this context, states are increasingly turning to OSINT for surveillance purposes, marking a notable trend. This practice presents specific challenges regarding human rights. These tools often involve potential violations of fundamental rights and are generally used outside the law. As this study will show, their use is typically unregulated, and where regulations do exist, they are insufficient.[13] Under broad and vague definitions, intelligence and security authorities monitor open sources of information on the internet, such as social media platforms, blogs, magazines, and newspapers. In some cases, the information obtained is organized, systematized, and incorporated into intelligence reports, which may include the profiling of citizens.

This report aims to provide an empirical approach and a comparative analysis of the use of OSINT by states in the region for surveillance purposes. It is a field study to understand the extent of these techniques' use, identify the actors employing them, and, if measurable, assess their impact and utility.

A consortium of organizations conducted this research, including Article 19 Brazil and South America, Article 19 Mexico and Central America, the Centro de Estudios en Libertad de Expresión y Acceso a la Información [Center for Studies on Freedom of Expression and Access to Information] (CELE), Datysoc, and Fundación Karisma. CELE led the coordination, which proposed an analytical-qualitative framework as the research methodology. The study began with an extensive review of the existing literature on the subject, the development of a common methodology, the submission of public information requests to state agencies, interviews with various actors from the public and private sectors in Argentina, Brazil, Colombia, Mexico, and Uruguay, and the drafting of five national reports.

Section II of this report defines some key concepts necessary for the research. Section III details the legal framework applicable to the practice of OSINT in each country where the study was conducted, particularly regarding its use by the state. This is because OSINT carried out by private actors is not the primary subject of this research and, in many cases, is covered by general regulations such as public access to information laws and personal data protection laws. Section IV describes the OSINT practices identified in each state, based either on the responses provided by state entities to the information requests or through interviews and press articles. Section V discusses the human rights impacts of state OSINT activities conducted for surveillance, mainly concerning privacy and freedom of expression. Finally, Section VI serves as the conclusion.

---

[13] See, for example, Resolution No. 144/2020 of the Ministry of Security of Argentina, repealed by resolution No. 720/ 2022.

II. OSINT and State Intelligence

Among the many changes that the internet has brought to contemporary societies, one of the most problematic is the increase in the State's surveillance capacity over its citizens.[14] Today, the amount of information available online about individuals is larger than ever. As that volume of information grows, the mechanisms for collecting, processing, and storing it become increasingly effective.

OSINT (the acronym for "Open-Source Intelligence") refers to "the practice involving the use of a set of techniques and technologies that facilitate the collection of information that is publicly available, such as texts, images, videos, audios, and even geospatial data. It is only when this information is given a specific purpose or use and linked to a concrete action that it becomes actual intelligence."[15][16*] It has also been defined as "intelligence produced from publicly available information that is collected, exploited, and disseminated promptly to an appropriate audience to address a specific intelligence requirement."[17] Information comes from various sources, such as books, newspapers, radio, television, government databases, publications on digital platforms, and in diverse formats such as text, photographs, videos, audio recordings, etc.

To understand exactly what we mean when we talk about OSINT, it is necessary to clarify the notions of "intelligence" and "open sources." The definitions of these concepts will be relevant when making distinctions and evaluating state conduct.

According to Peter Gill and Mark Phythian, intelligence is the set of "activities –generally secret– of targeting, collection, analysis, dissemination, and action, intended to enhance security and/or maintain relative power vis-à-vis competitors through the early detection of threats and opportunities."[18] Although other definitions are possible, this one is useful because it highlights several elements common to all intelligence activities: first, the fact that it is generally carried out in secret, second, the existence of a specific purpose, and third, its function of early or

---

[14] United Nations (UN), Human Rights Council, "El derecho a la privacidad en la era digital," Report of the United Nations High Commissioner for Human Rights, A/HRC/27/37, June 30, 2014, § 2.

[15] ADC (n. 7), p. 5.

[16*] TN Source Language Note: All legal citations were originally in Spanish unless specified otherwise, with the exception of Brazil-related sections (Portuguese originals). English translations derive from existing Spanish versions of the source materials.

[17] Office of the Director of National Intelligence, "U.S. National Intelligence: An Overview 2011," 2011, p. 54, quoted in Williams, Heather J., and Ilana Blum, "Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise," RAND Corporation, 2018, p. 1.

[18] Gill, Peter and Phythian, Mark, Intelligence in an Insecure World, Cambridge, Polity Press, 3rd ed., 2018, p. 19, quoted in Omand, David and Phythian, Mark, Principled Spying: The Ethics of Secret Intelligence, Oxford, Oxford University Press, 2018, p. 10.

preventive detection. Many of the activities presented by governments in the region as "cyber-patrolling" share these characteristics and are, strictly speaking, intelligence activities. Finally, it is important to explain that "intelligence" refers both to the cycle of actions mentioned and to the resulting product. OSINT is one of the various sources or disciplines of intelligence collection, alongside SIGINT,[19] COMINT,[20] HUMINT,[21] and GEOINT.[22]

Once OSINT has been defined and situated within the framework of intelligence activity, we need to define "open source." First, it is worth noting that "open sources" include both offline information (from traditional media such as television, radio, newspapers, academic publications, and libraries) and online sources. The concept of OSINT, therefore, predates the internet. Consequently, the category of "open sources" encompasses different types of information accessible through various channels.[23]

This study will focus particularly on the use of open sources on the internet by the State for surveillance. This activity presents a number of unique characteristics. First, the rapid growth of the web has caused the volume of available and analyzable information to increase exponentially. This, in turn, has led to the rapid development of technological tools to massively collect, analyze, and classify that information.

The use of OSINT for surveillance has become widespread, and states have "normalized" its application. It has even been presented to the public as a legitimate tool for internal security under the name of "cyber-patrolling." This has been done without informing the population about its potential impact on human rights.[24]

---

[19] SIGINT involves gathering information by intercepting a wide range of signals (e.g., radar, telephone communications, or other systems). For further information, see Office of the Director of National Intelligence, "What is Intelligence?" retrieved from: https://www.dni.gov/index.php/what-we-do/what-is-intelligence, last access: August 9, 2023.

[20] COMINT refers to information collected from individuals' communications including phone conversations, text messages, and other online interactions. Tech Target, (n. 3).

[21] HUMINT is the term used for the collection of information from human sources. It does not necessarily involve espionage or covert activity; most HUMINT is produced by non-covert individuals, such as strategic informants, military attachés, etc. See more in Office of the Director of National Intelligence, (n. 17).

[22] GEOINT consists of the analysis and visual representation of security-related activities on the ground. It is produced through the integration of imagery, imagery intelligence, and geospatial information. See more in Office of the Director of National Intelligence, (n. 17).

[23] Bertoni, Eduardo, "¿Las prácticas OSINT son amigas o enemigas de los derechos humanos?" 2022 (pending publication).

[24] Fundación Karisma, "El Estado monitorea internet: implicaciones en los derechos humanos del ciberpatrullaje," 2023, retrieved from: https://web.karisma.org.co/el-estado-monitorea-internet-implicaciones-en-los-derechos-humanos-del-ciberpatrullaje, last access: August 9, 2023.

These impacts relate, first and foremost, to individuals' right to privacy. Unlike information formerly obtained from mass media, books, or other analog publications, information extracted from the web may not be intended for mass dissemination. Moreover, in the vast majority of cases, the amount of information available online about a person is far greater than what exists offline, and the methods used to collect it may be disproportionate in relation to the needs of the state and its purposes.

Finally, one must also consider the possible chilling effect that the widespread use of OSINT by the State may have on internet users, potentially having a significant impact on the right to freedom of expression — both in its individual and collective dimensions.

III. Legal Framework

III.1. Argentina

III.1.a. National Laws

The activities of intelligence agencies in Argentina are regulated by the National Intelligence Law (No. 25,520),[25] which establishes the inviolability of communications and documents that are "private or of unauthorized access or reading, or not accessible to the public."[26] Meanwhile, the National Defense Law (No. 23,554)[27] prohibits the Armed Forces from carrying out intelligence tasks related to the country's internal politics.[28] The law does not specify the nature of the intelligence

[25] Información Legislativa (Infoleg), Ministry of Justice and Human Rights, Office of the President, Ley de Inteligencia Nacional No. 25,520, retrieved from: http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/texact.htm, last access: August 9, 2023.

[26] Article 5: "Throughout the Republic of Argentina, all telephone, postal, telegraph, or facsimile communications, or any other system for sending objects or transmitting images, voices, or data packets, as well as any type of private information, files, records, and/or documents not authorized for access or reading or not accessible to the public are inviolable, except when a court order or authorization provides otherwise."

[27] Infoleg, Ministry of Justice and Human Rights, Presidency of the Nation, Internal Security, "Principios básicos. Finalidad y estructura del sistema. Organización de las Fuerzas Armadas. Servicio de Defensa Nacional. Organización Territorial y Movilización. Disposiciones generales y transitorias," Law No. 23,554, retrieved from: http://servicios.infoleg.gob.ar/infolegInternet/anexos/20000-24999/20988/texact.htm, last access: August 14, 2023.

[28] "Matters related to the internal politics of the country may under no circumstances constitute working hypotheses for military intelligence agencies" (Art. 15) Finally, according to Article 4, "the fundamental difference between National Defense and Internal Security must be permanently observed."

tasks allowed; however, the National Defense System's operations are limited to the prevention and management of conflict scenarios.[29]

III.1.b. The "Cyber Patrol Protocol" of the Ministry of Security

Currently, there is no specific protocol regulating the practice of OSINT by security forces or intelligence agencies. However, between 2018 and 2022, two protocols were issued that sought to regulate it within the scope of security force activities.

On July 26, 2018, the Security Secretariat of the National Ministry of Security issued Resolution No. 31/2018, which authorized national internal security forces to conduct OSINT in relation to crimes such as the illegal sale of weapons online or of any item that could originate from the commission of a crime or customs violations, the dissemination of images potentially linked to human trafficking and smuggling, and the online sexual harassment of minors.

The resolution also established that "investigative actions must be limited to publicly accessible sites, with a particular focus on social networks of any kind, sources, public and open databases, websites, the dark web, and other relevant publicly accessible sites."[30] The OSINT activities carried out under this regulation were intended to gather the necessary evidence to file a complaint with the appropriate judicial authorities.

Although this investigation accessed the resolution, it was never officially published in the Boletín Oficial (Official Gazette)[31] and only became publicly known during the debate preceding the adoption of Resolution No. 144/2020, which repealed it.

Between May 31, 2020, and October 31, 2022, the "Protocolo General para la Prevención Policial del Delito con Uso de Fuentes Digitales Abiertas [General Protocol for Police Crime Prevention Using Open Digital Sources] was in effect. This protocol, approved by Resolution No. 144/2020 of the National Ministry of Security,[32] repealed Resolution No. 31/2018. It aimed to "establish principles, criteria, and general guidelines for crime prevention tasks carried out in cyberspace by police

---

[29] The activity of the National Defense System is confined by Article 3 of the aforementioned law to "the set of plans and actions aimed at preventing or overcoming conflicts generated by such aggressions, both in times of peace and war, managing all aspects of the Nation's life during the conflict, and consolidating peace once the hostilities have ended."

[30] Author emphasis.

[31] This is according to official sources. Infoleg, Ministry of Justice and Human Rights, Presidency of the Nation, Ministry of Security, resolution No. 144/2020, retrieved from:
http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=338229, last access: August 9, 2023.

[32] Ibid.

forces and security forces under the jurisdiction of the Ministry of Security."[33] Its scope covered specific crimes related to the COVID-19 pandemic.

Finally, on October 27, 2022, the National Ministry of Security issued Resolution No. 720/2022,[34] ordering the repeal of Ministerial Resolution No. 144 of May 31, 2020, along with its complementary regulations. In response to a public information request from CELE, the National Ministry of Security reported that the repeal of Resolution No. 144/2020 did not reinstate Resolution No. 31/2018.

III.1.c. Police of the Autonomous City of Buenos Aires

In Buenos Aires, Article 89 of the Ley del Sistema Integral de Seguridad Pública de la Ciudad Autónoma de Buenos Aires [Law on the Comprehensive Public Security System of the Autonomous City of Buenos Aires] (No. 5,688)[35] grants the City Police the power to conduct criminal intelligence tasks, but only within the framework of judicial proceedings.

III.2. Brazil

Article 144 of Brazil's Federal Constitution establishes public security as the protection of "public order and the safety of individuals and property," enforced by agencies such as the Federal Police, Federal Highway Police, Civil Police, Military Police, military fire departments, and Federal/State Criminal Police.

Law No. 13,675/2018[36] establishes the Unified Public Security System (SUSP) and creates the National Public Security and Social Defense Policy (PNSPDS).[37] The guidelines of the PNSPDS include the "systematization and exchange of information on citizen security, prison systems, and drugs at the national level" and the "use of an integrated electronic information and data system."

---

[33] Ibid., Art. 1.

[34] Infoleg, Ministry of Justice and Human Rights, Presidency of the Nation, Ministry of Security, resolution No. 720/2022, retrieved from: http://servicios.infoleg.gob.ar/infolegInternet/anexos/370000-374999/373942/norma.htm, last access: August 9, 2023.

[35] Buenos Aires Cuidad, "Digesto G.C.B.A. - Detalle de la norma," 2018, retrieved from: https://digesto.buenosaires.gob.ar/buscador/ver/25729, last access: August 9, 2023.

[36] Presidency of the Republic, General Secretariat, Subdirectorate of Legal Affairs, Law No. 13,675, 2018, retrieved from: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13675.htm, last access: August 9, 2023.

[37] Decree No. 9,489/2018 regulates, at the Union level, Law No. 13,675/2018, which establishes the rules, structure, and procedures for implementing the National Public Security and Social Defense Policy. Decree No. 9,489, 2018, retrieved from: https://dspace.mj.gov.br/bitstream/1/2221/4/DEC_2018_9489.htm, last access: August 9, 2023.

Law No. 9,883/1999[38] establishes the Brazilian Intelligence System and creates the Brazilian Intelligence Agency (ABIN). This law defines intelligence as "the activity aimed at obtaining, analyzing, and disseminating knowledge within and outside the national territory about facts and situations that have an immediate or potential influence on governmental decision-making and actions, and the safeguarding and security of society and the state."

Decree No. 3,695/2000[39] created the Public Security Intelligence Subsystem (SISP) within the scope of the Brazilian Intelligence System. According to the decree, the Subsystem members must "identify, monitor, and assess real or potential threats to public security and generate knowledge and information to support actions to neutralize, curb, and repress criminal acts of any nature." The SISP was regulated by Resolution No. 1 of July 15, 2009, issued by the National Secretariat of Public Security, which defined the roles and scope of intelligence agencies. Although the regulation does not specifically mention open-source intelligence, it does refer to the use of information and data and their corresponding strategic processing.[40]

Finally, it is worth mentioning the Secretariat for Integrated Operations (SEOPI), which falls under the Ministry of Justice and Public Security, created by Decree No. 9,662/2019, regulated by Decree No. 11,103/2022,[41] and subsequently dissolved by Decree No. 11,348/2023.[42] The SEOPI was responsible for, among other functions: i) advising the Minister on intelligence activities and police operations, with a focus on integration with international, federal, state, municipal, and district organizations, as well as public security bodies; ii) implementing, maintaining, and modernizing integration networks and national public security intelligence systems; and iii) promoting the integration of public security intelligence activities, in line with the federal, state, municipal, and district intelligence agencies that make up the Public Security Intelligence Subsystem. The same decree establishes that the Directorate of Intelligence (Article 32) is responsible for: i) promoting, with the constituent bodies of the Brazilian Intelligence System, the exchange of data and knowledge necessary for

---

[38] Presidency of the Republic, Casa Civil, Subdirectorate of Legal Affairs, Law No. 9,883, 1999, retrieved from: http://www. planalto.gov.br/ccivil_03/leis/L9883.htm, last access: August 9, 2023.

[39] Presidency of the Republic, General Secretariat, Subdirectorate of Legal Affairs, Decree No. 3,695, 2000, retrieved from: http://www.planalto.gov.br/ccivil_03/decreto/d3695.htm, last access: August 9, 2023.

[40] According to Article 7 of Resolution No. 1 of July 15, 2009.

[41] Presidency of the Republic, General Secretariat, Subdirectorate of Legal Affairs, Decree No. 11,103, 2022, retrieved from: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Decreto/D11103.htm, last access: August 9, 2023.

[42] Presidency of the Republic, General Secretariat, Subdirectorate of Legal Affairs, Decree No. 11,348, 2022, retrieved from: http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11348.htm, last access: August 9, 2023.

administrative and operational decision-making of the Secretariat of Integrated Operations; and ii) planning, supervising, and executing actions related to the collection and analysis of data for the production of public security intelligence knowledge intended to advise the Secretariat of Integrated Operations.

III.3. Colombia

Resolution No. 5,839/2015 of the Colombian National Police authorizes the Police Cyber Center, which is part of the division responsible for judicial investigations, to:

> carry out 24/7 cyber-patrolling on the web to identify threats originating from or directed toward Colombia that affect citizen cybersecurity, developing the capacity to identify and detect common factors in known incidents, as well as breaches of the availability, integrity, and confidentiality of the information circulating in cyberspace.[43]

Law No. 906 of 2004 of the Code of Criminal Procedure establishes in Article 242B the possibility for officials of the Office of the Attorney General of the Nation—the body responsible for investigating criminal offenses in Colombia—to conduct "undercover operations in virtual communication media" in investigations related to organized crime in which "there is verification of the possible existence of acts constituting crimes committed by criminal organizations that operate through communications maintained on closed virtual communication channels." In all cases, prior authorization from the Judge for the Control of Guarantees is required.

The Intelligence Law (No. 1,621/2013) establishes that the only entities authorized to carry out intelligence and counterintelligence tasks are "the divisions of the Military Forces and the National Police organized for that purpose, and the Financial Information and Analysis Unit (UIAF)."[44] Additionally, Article 4 subjects intelligence activity to the "principle of legal confidentiality, which guarantees the protection of the rights to honor, good name, personal and family privacy, and due process."[45] The same article prohibits intelligence information from being "collected, processed, or disseminated on the basis of gender, race, national or family origin, language, religion, political or philosophical opinion, membership in a union, social or human rights

---

[43] Ministry of National Defense, National Police, General Directorate, resolution No. 5,839, "Por la cual se define la estructura orgánica interna de la Dirección de Investigación Criminal e INTERPOL, se determinan las funciones de sus dependencias y se dictan unas disposiciones," 2015, retrieved from: https://www.policia.gov.co/file/32305/download?token=OA0OIAOJ, last access: August 17, 2023.

[44] Law No. 1,621/2013, Article 3.

[45] Ibid., Article 4.

organization, or to promote the interests of any political party or movement, or to affect the rights and guarantees of opposition political parties."[46] Article 5 mandates that intelligence activity be subject to the principles of necessity, suitability, and proportionality.[47]

III.4. Mexico

"Cyber-patrolling" actions were included in the "Modelo homologado de las unidades de policía cibernética" [Standardized Model for Cyber Police Units], established by Agreement 06/XLI/16, approved on December 20, 2016, by the National Public Security Council. The model serves as a guide for the cyber police forces of the states within the union and is part of the "detection and timely response to cybercrime" component of the National Public Security Program (2013–2018) of the Enrique Peña Nieto administration. It details the tasks of "cyber-patrolling" as aimed at:

> identifying likely behaviors constituting cybercrimes committed online through the search for data in public sources that allow for the generation of intelligence and new lines of investigation in collaboration with other police units and institutions at all three levels of government (municipal, state, and federal) and the relevant authorities.[48]

After Andrés Manuel López Obrador came to power in 2018, the Federal Police was replaced by the National Guard (GN). Its Organic Law states that the GN has the authority to "monitor, identify, track, and surveil the public internet network and websites, under the guise of preventing criminal behavior."[49]

Additionally, in October 2020, the Secretariat of Security and Citizen Protection (SSPC), through the Executive Secretariat of the National Public Security System (SESNSP) and the National Information Center (CNI)[50] introduced the

---

[46] Ibid.

[47] Law No. 1,621/2013, Article 5.

[48] Author emphasis. Government of Mexico, "Modelo homologado de unidades de policía cibernética," retrieved from: https://www.gob.mx/cms/uploads/attachment/file/189189/Modelo_homologado_unidades_policia_cibernetica.pdf, last access: August 9, 2023.

[49] Author emphasis. Article 9, section XXXVIII of the Ley de la Guardia Nacional, passed on May 27, 2019.

[50] The Centro Nacional de Información [National Information Center] (CNI) is a decentralized body under the Secretariat of Security and Citizen Protection (SSPC). It carries out intelligence tasks to safeguard the integrity, stability, and continuity of the Mexican State (Article 19, Ley de Seguridad Nacional [National Security Law]).

"Multi-Source System for estimating crime incidence, aimed at police intelligence" (hereinafter "multi-source system") as part of the strengthening of the "National Model for Police and Civic Justice."[51] The Multi-Source System was designed to reduce unreported crime (cifra negra) and support police intelligence by incorporating "ten solid and complementary sources," including data analysis and actionable intelligence from open sources (OSINT).[52]

Despite the legal authorizations, the agencies that carry out "cyber-patrolling" do not publish information about their activities. As a result, there is no transparency regarding what information is sought and collected, under what circumstances, and how that information is processed.

III.5. Uruguay

The operation of intelligence agencies in Uruguay is governed by Law No. 19,696 of the National Intelligence System (SNIE Law).[53] In Article 3, this regulation defines open sources as "those from which a given report can be obtained with no restriction other than the effort required to obtain it," as opposed to closed sources, which it defines as "those whose access is restricted and for which obtaining the information requires the use of special means and procedures."

Article 3, Paragraph E of the Intelligence Law defines police intelligence as "an activity that includes the collection, processing, analysis, and distribution of information related to the prevention and potential suppression of common crime and organized crime, serving as an auxiliary to the Judiciary through the prevention and suppression of crime." This definition merges the concept of police intelligence with crime suppression activities, which poses a potential risk of expanding the use of intelligence

---

[51] The National Police and Civic Justice Model was approved on July 8, 2019. Government of Mexico, "Modelo Nacional de Policía y Justicia Cívica," 2020, retrieved from: https://www.gob.mx/sesnsp/articulos/modelo-nacional-de-policia-y-justicia-civica-238637, last access: August 9, 2023.

[52] Government of Mexico, "Presentan SSPC-SESNSP Sistema Multifuente para la incidencia delictiva," 2020, retrieved from: https://www.gob.mx/sspc/prensa/presentan-sspc-sesnsp-sistema-multifuente-para-la-incidencia-delictiva, last access: August 9, 2023.

[53] Centro de Información Oficial, Normativa y Avisos Legales Uruguay, Law No. 19,696, 2018, retrieved from: https://www.impo.com.uy/bases/leyes/19696-2018, last access: August 9, 2023.

reports and technologies within crime prevention and suppression activities and the sphere of criminal proceedings.

In turn, Article 20 of the SNIE Law[54] establishes that certain information-gathering operations constitute "special procedures that may affect the freedom and privacy of citizens" and therefore require prior authorization from the Judiciary. The law defines special procedures as "those that allow access to relevant background information contained in or originating from closed sources." Thus, we find that the concept of "special procedures" applies only to "closed" sources, so prior judicial authorization would not be required to conduct OSINT.

For its part, the Intelligence Law authorizes personnel of the agencies that constitute the National State Intelligence System to carry out undercover activities "to obtain background information and intelligence" with prior written authorization from their authorities. This includes "the possible issuance of any necessary documents to protect the identity of the personnel involved." It follows that the Uruguayan Intelligence Law would also not require a court order to create false profiles (Article 21 of the Intelligence Law); written authorization from the administrative authority of an agency within the SNIE would be sufficient. There is also no legal regulation of the procedures and timelines for such operations, nor of the control systems or reporting obligations of these undercover agents.

Finally, Article 7 of the law prohibits agencies from conducting repression or criminal investigation activities on their own "unless such activity falls within their specific legal mandates."[55] Thus, the prohibitions in Article 7 do not address the problems arising from the broad and ambiguous definition of police intelligence.

---

[54] Ibid.

[55] "No intelligence agency shall have coercive powers, and shall be specifically prohibited from: 1) carrying out repressive tasks; performing, on their own, police functions or criminal investigation, unless such activity falls within their specific legal mandates or is requested by a court order within the framework of a specific case."

Meanwhile, the definition of "public sources" in the Personal Data Protection Law (No. 18,331) does not include the internet.[56] The Regulatory and Supervisory Unit for Personal Data (URCDP) does not consider the internet to be a public source.[57] However, this limited scope that the Personal Data Protection Law gives to the concept of "public sources" is not clearly applicable to the processing of personal data for intelligence and public security purposes. This is because Article 3, Section B,[58] and Article 25[59] of that law exclude from its scope the "processing of personal data for national defense or public security purposes" by the armed forces, police agencies, or intelligence services, provided that "they are necessary for the strict fulfillment of legally assigned missions for national defense, public security, or crime suppression."

Professor Rodrigo Rey raises serious criticisms of the SNIE Law and highlights that "it is subject to significant objections (we believe there are arguments supporting the potential unconstitutionality of certain provisions) in terms of legislative technique, and particularly, these concerns extend to the unclear lines between the production of

---

[56] "Article 9 bis (...) the following sources or documents shall be considered public or accessible to the public: a) the Official Gazette and official publications, regardless of their storage format or communication channel. b) Publications in mass media, meaning those from the press, regardless of the medium in which they are published or the channel through which the communication is carried out. c) Directories, yearbooks, listings, and similar publications that include names and addresses or other personal data, provided such data were included with the consent of the data subject. d) Any other record or publication in which the public interest prevails in that the personal data contained therein may be consulted, disseminated, or used by third parties. Otherwise, the record or publication may be used through techniques of dissociation or anonymization of personal data."

[57] In its opinion No. 10/020 dated June 23, 2020, the Unidad Reguladora y de Control de Datos Personales [Regulatory and Control Unit for Personal Data] (URCDP) stated that "Article 9 bis of Law No. 18,331 does not include the internet in the list of public or publicly accessible sources, and therefore, company data found on Yellow Pages or other websites are not considered public or publicly accessible data simply by being published there." See Government of Uruguay, Unidad Reguladora y de Control de Datos Personales, Opinion No. 10/020, 2020, retrieved from: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/dictamen-n-10020, last access: August 9, 2023.

[58] "Article 3. (...) This law shall not apply to the following databases: (...) b) Those intended for public safety, defense, state security, and its activities related to criminal matters, investigation, and crime suppression."

[59] "Article 25. Databases corresponding to the Armed Forces, police agencies, or intelligence services. (...) The processing of personal data for national defense or public security purposes by the Armed Forces, police agencies, or intelligence services without prior consent of the data subjects is limited to those cases and categories of data that are necessary for the strict fulfillment of the missions legally assigned to them for national defense, public security, or crime suppression. The databases, in such cases, must be specific and established for that purpose and classified by categories based on their degree of reliability.
Personal data recorded for police purposes shall be erased when they are no longer necessary for the investigations that justified their storage."

intelligence information and investigative or prosecutorial activities."[60] In addition to the shortcomings related to the very definition of police intelligence, Rey also criticizes the lack of regulation regarding the design of information-gathering procedures, their management, and the possibility of accessing such data:

> This results in administrative agencies, rather than the legislator, determining the events that justify intelligence activities. In other words, there is no minimum legal standard for justification, which can lead to blatant partiality. Additionally, there are no defined terms or deadlines for decision-making, no established appeal mechanisms, and no provisions for extensions, which could otherwise serve as an effective oversight mechanism to review the specific content collected and assess its relevance.[61]

IV. Requests for Access to Information and Observed Practices

IV.1. Argentina

From the responses to public information access requests submitted in Argentina to various public agencies, only the Buenos Aires City Police and the Anti-Corruption Office, which reports to the national Executive Branch, stated that they use OSINT tools. The Buenos Aires City Police reported that "it has a unit called Cyber Patrol, which performs various tasks of open source analysis on public social media, under judicial order."

The Anti-Corruption Office stated that the Complaints Admission and Referral Coordination Department does not collect information but "accesses information through open or semi-open databases to resolve each case under review, which are duly added to the electronic files that initiate the searches." Subsection (e) of Article 2 of

[60] Rey, Rodrigo, "La regulación del Sistema Nacional de Inteligencia de Estado, y una lectura introductoria sobre los procedimientos especiales de obtención de información," in: Revista de Derecho Penal, No. 27, 2019, pp. 19-41, retrieved from: https://revistas.fcu.edu.uy/index.php/penal/article/view/1915, last access: August 9, 2023.
[61] Ibid.

Annex I of Resolution MJSyDH No. 1,316/08 supports this investigative activity, according to the agency."[62]

The other agencies consulted — except the Federal Intelligence Agency, which did not respond to the information access requests— replied that they do not conduct OSINT and have also not entered into contracts with private companies to obtain OSINT services or software that facilitates such tasks. However, from consulting publications in the press and interviews with specialists in the field and people who practice or have practiced OSINT, we have verified various instances in which the State has carried out OSINT for surveillance purposes.

IV.1.a. The National Ministry of Security

In April 2020, during the COVID-19 pandemic, then-Minister of Security Dr. Sabina Frederic publicly referred to the existence of a "cyber-patrolling" plan aimed at "measuring social sentiment," based primarily on the monitoring of open sources, social media in particular,[63] which led to the adoption of Resolution No. 144/2020.

In 2016, the Argentine Federal Police raided the home of Nicolás Lucero, a 19-year-old resident of José León Suárez (Buenos Aires Province). Following the raid, Nicolás was taken to a police station, where officers seized his and his family's cell phones, as well as his sister's netbook.[64] He was charged with the crime of public intimidation following

---

[62] Article 2 of Resolution MJSyDH No. 1.316/08 (the internal regulations of the Investigations Directorate of the Anti-Corruption Office) reads: "Article 2.- Once a proceeding has been initiated, the Administrative Oversight Prosecutor shall decide, in the exercise of the authority granted by Article 8, subsection (e) of Decree No. 102/99: (...) e) Before taking any of the actions described above, both the Administrative Oversight Prosecutor and the Director of Investigations, or any of the Administrative Investigators (with the knowledge of the Administrative Oversight Prosecutor), may carry out preliminary evidentiary measures to clarify the description of a fact, to determine whether it falls within the jurisdiction established by Article 1 of Decree No. 102/99 or exceeds the significance criteria outlined in the Office's Action Plan."

[63] See Infobae. "Polémica revelación: la ministra de Seguridad admitió que las fuerzas a su cargo realizan ciberpatrullaje en redes sociales para "detectar el humor social," 2020, retrieved from: https://www.infobae.com/politica/2020/04/09/polemica-revelacion-la-ministra-de-seguridad-admitio-que-las-fuerzas-a-su-cargo-realizan-ciberpatrullaje-en-redes-sociales-para-detectar-el-humor-social, last access: August 9, 2023.

[64] Lamas, Federico, "La increíble historia detrás del tuit contra Macri que terminó en la Justicia," Diario Popular, 2017, retrieved from: https://www.diariopopular.com.ar/general/la-increible-historia-detras-del-tuit-contra-macri-que-termino-la-justicia-n327253, last access: August 9, 2023.

a tweet,[65]sarcastic in tone, referring to the then-President of the Nation. Nicolás had to face criminal proceedings, in which he was acquitted by the courts in 2018.[66]

In a similar situation, in April 2020, Kevin Guerra, a 20-year-old from the town of Junín in the province of Buenos Aires, posted a tweet in which he joked about the delays in receiving emergency aid provided by the national government during the COVID-19 pandemic.[67] The National Gendarmerie (under the Ministry of Security) flagged the tweet as part of its 'social media cyber-patrolling operations' and initiated criminal proceedings against Kevin. The judicial case was classified as "public intimidation."[68] Kevin was ultimately acquitted. According to the Centro de Estudios Legales y Sociales [Center for Legal and Social Studies] (CELS), which took on his defense, the tweet in question was identified through a search conducted by the National Gendarmerie using the terms "loot, quarantine, and Argentina." The Gendarmerie based its actions on the authorization provided by Resolution No. 31/2018 of the National Ministry of Security.[69]

Finally, it is important to mention the raids on "social media agitators" conducted in April 2020 simultaneously in various locations across the province of Buenos Aires. During that operation, homes were raided, and cell phones and computers were seized from several individuals who, according to the Ministry of Security, had allegedly "incited the commission of crimes" using fake social media profiles.[70]

---

[65] See https://twitter.com/nicolucero69/status/765936986217668608, last access: August 18, 2023.
[66] Diario Perfil, "Declaran 'inocente' al joven que estuvo preso por un tuit contra Mauricio Macri," 2018, retrieved from: https://www.perfil.com/noticias/sociedad/declaran-inocente-al-joven-que-escribio-un-tuit-contra-macri.phtml, last access: August 9, 2023.
[67] Retrieved from: https://twitter.com/KevinGuerra99/status/1247709948554903554, last access: August 9, 2023.
[68] Diario Ámbito, "Habló Kevin Guerra, detenido por twittear: 'Todo esto fue un chiste'," 2020, retrieved from: https://www.ambito.com/informacion-general/bono/hablo-kevin-guerra-detenido-twittear-todo-esto-fue-un-chiste-n5095854, last access: August 9, 2023.
[69] Centro de Estudios Legales y Sociales (CELS), "La justicia federal sobreseyó a Kevin Guerra por sus expresiones en Twitter," 2021, retrieved from: https://www.cels.org.ar/web/2021/01/la-justicia-federal-sobreseyo-a-kevin-guerra-por-sus-expresiones-en-twitter, last access: August 9, 2023.
[70] A24, "En medio de la pandemia por coronavirus, se realizaron 20 allanamientos contra agitadores en las redes sociales," 2020, retrieved from: https://www.a24.com/policiales/medio-pandemia-coronavirus-realizaron-20-allanamientos-agitadores-redes-sociales-09042020_umqdiP2qx, last access: August 9, 2023.

IV.1.b. Ministry of Foreign Affairs

Reports indicate that ahead of the 2017 and 2018 WTO and G20 meetings in Argentina, the Federal Intelligence Agency (AFI)—at the request of the Ministry of Foreign Affairs—conducted illegal profiling of journalists, academics, and civil society members seeking accreditation or planning to attend. The profiling was used to assess whether their participation would be permitted.[71] Based on these profiles, 65 individuals were denied accreditation, and several foreign nationals who attempted to enter the country despite rejection were deported.[72]

In an official statement, the Ministry of Foreign Affairs claimed that those denied accreditation had " publicly incited violence on social media, declaring their intention to provoke intimidation and chaos."[73] The Ministry's statements confirm that open-source intelligence gathering was used for political profiling—a practice explicitly banned under the Intelligence Law.

IV.1.c. Federal Administration of Public Revenue

In November 2022, following an investigation published in the press,[74] it came to light that the Federal Administration of Public Revenue (hereinafter, AFIP)—the national government's tax collection agency— filed a complaint with a prosecutor's office specializing in cybercrime regarding the activity of individuals who were allegedly offering fraudulent waybills [cartas de porte] (a mandatory electronic document

---

[71] Diario Ámbito, "Piden la indagatoria de Arribas y Majdalani por espionaje ilegal en las cumbres de la OMC y el G20," 2021, retrieved from:
https://www.ambito.com/politica/espionaje/piden-la-indagatoria-arribas-y-majdalani-ilegal-las-cumbres-la-omc-y-el-g20-n5180581, last access: August 9, 2023.

[72] CELS, "Reunión de la OMC en la Argentina: acreditaciones rechazadas y deportaciones," 2017, retrieved from:
https://www.cels.org.ar/web/2017/12/wto-meeting-in-argentina-rejected-accreditations-and-deportations, last access: August 9, 2023.

[73] Author emphasis. It was not possible to access the original statement. The quoted text corresponds to the screenshot shown, which was obtained from the CELS website and can be found in the Ministry of Foreign Affairs, International Trade and Worship, Argentina, "Sobre la acreditación de ONG's a la Conferencia Ministerial de la OMC en Buenos Aires," 2017, retrieved from:
https://cancilleria.gob.ar/es/actualidad/comunicados/sobre-la-acreditacion-de-ongs-la-conferencia-ministerial-de-la-omc-en-buenos, last access: August 9, 2023.

[74] Martínez, Belkis, "'Estafa': venden por $500.000 un documento clave de la AFIP," Diario La Nación, 2022, retrieved from:
https://www.lanacion.com.ar/economia/campo/estafa-venden-por-500000-un-documento-clave-de-la-afip-nid29112022, last access: August 9, 2023.

issued by AFIP that authorizes the transport of grains by road and rail) on social media. Upon receiving the information and before filing the complaint, "the División Penal Tributaria [Tax Criminal Division] [of AFIP] conducted investigative tasks on open social media sites, identifying various profiles and posts on the Facebook platform where these documents were being offered to simulate transactions, but noted that they were unable to obtain data."[75]

IV.1.d. Federal Intelligence Agency

The Federal Intelligence Agency did not respond to the request for public information submitted for this investigation. However, this agency has been confirmed to have carried out OSINT activities.

In 2020, the then-comptroller of the AFI reported finding folders at the Agency's headquarters containing intelligence files on journalists, politicians, civil society organizations, and academics.[76] A source from the Federal Intelligence Agency stated to the press that "although the journalists' files are based on open sources, such as social media, the Intelligence Law prohibits the collection of this information."[77] Many of these files had been created during the accreditation process before the WTO and G20 meetings in Argentina in 2017 and 2018, respectively. After the change of administration, the Agency handed over the intelligence files it had produced to the

---

[75] Martínez, Belkis, "La AFIP presentó una denuncia por la supuesta venta ilegal y millonaria de un documento clave," Diario La Nación, 2022, retrieved from: https://www.lanacion.com.ar/economia/campo/la-afip-presento-una-denuncia-por-la-supuesta-venta-ilegal-y-millonaria-de-un-documento-clave-nid05122022/, last access: August 9, 2023.

[76] Pizzi, Nicolás, "La AFI denunció ante la Justicia que durante el gobierno de Mauricio Macri se hizo inteligencia ilegal contra organizaciones sociales y periodistas," Diario Infobae, 2020, retrieved from: https://www.infobae.com/politica/2020/06/05/la-afi-denuncio-ante-la-justicia-que-durante-el-gobierno-de-mauricio-macri-se-hizo-inteligencia-ilegal-contra-organizaciones-sociales-y-periodistas, last access: August 9, 2023.

[77] Author emphasis. Pizzi, Nicolás, "Las fichas de inteligencia que elaboró la AFI durante el gobierno de Macri sobre las personas que asistieron a las cumbres del G20 y la OMC," Diario Infobae, 2020, retrieved from: https://www.infobae.com/politica/2020/06/07/que-dicen-las-fichas-que-armaba-la-afi-en-la-previa-del-g20-y-la-reunion-de-la-omc-en-buenos-aires, last access: August 9, 2023.

affected individuals.[78] The use of OSINT and other forms of intelligence to build their profiles can be observed there.

IV.1.e. Police of the Autonomous City of Buenos Aires

The Buenos Aires City Police claimed in its response to a public information request, filed as part of this investigation, that its Cyber-Patrolling unit conducts OSINT operations exclusively under court order. Documented evidence demonstrates the unit's participation in at least two instances exceeding the bounds of this claimed legal framework.

In July 2016, the Buenos Aires City Police arrested two young individuals who had posted threats against then-President Mauricio Macri on the social network Twitter. The post consisted of the caption "See you soon, @mauriciomacri," accompanied by an image of explosives and inscriptions in Arabic. The Secretary of Security of the Buenos Aires government, Marcelo D'Alessandro, stated to the press that the two people detained for these messages "are an example that we are vigilant about this type of incident, which seeks to instill fear in the population, and that we have the technology and determination needed to find those responsible without delay."[79] The press report from which this information was obtained also indicated that personnel from the National Ministry of Security participated in the investigation.

Furthermore, the investigation included an interview with a former security force operative involved in open-source intelligence (OSINT) activities.[80] He stated that the searches were carried out at the request of the Judiciary and that they involved collecting 'information about people in general,' which includes information about identified individuals. Regarding the procedure, they explained that "there is an informal process that somewhat depends on the Judiciary's discretion. The protocol is similar to when my son wants to find out who his ex is hanging out with. They look at

---

[78] A journalist from Perfil Publishing shared the contents of the file that the AFI had compiled about him. See Recalt, Rodis, "Exclusivo: las carpetas del espionaje," Revista Noticias, 2021, retrieved from: https://noticias.perfil.com/noticias/politica/exclusivo-las-carpetas-del-espionaje.phtml, last access: August 9, 2023.

[79] Diario Clarín, "Amenazaron con mensajes en árabe que iban a atentar contra Macri," 2016, retrieved from: https://www. clarin.com/policiales/amenazaron-mensajes-arabe-atentar-macri_0_SJNELzqO.html, last access: August 9, 2023.

[80] Interview conducted on October 27, 2022. The interviewee requested to remain anonymous.

the person's profile picture and then check all their social media until they figure out who they are, who they associate with, etc." Finally, they reported that the City Police interprets Article 10 of Law No. 5,847 on the Régimen Integral para Eventos Futbolísticos [Comprehensive Framework for Football Events] as authorizing OSINT practices. This article establishes the Database on Violence at Football Events in CABA and states that:

> The competent authority, acting under its preventive powers, must also deny access and presence at venues to individuals who, based on reasonable, objective criteria, are deemed likely to disrupt public order during a football event. This preventive determination must be communicated to the involved entity so that it may express its intent to exercise the right of admission for future football events.

IV.2. Brazil

As part of this study, several public information access requests were submitted to various Brazilian state agencies. The Navy Intelligence Center, the Brazilian Intelligence Agency (ABIN), and the Federal Police declined to respond, citing the nature of intelligence activities or invoking security concerns.

IV.2.a. Federal Public Prosecutor's Office

The Federal Public Prosecutor's Office reported that all areas of the Secretariat for Expertise, Research, and Analysis (SPPEA) collect data from open sources. In this regard, civil society has already raised concerns about the use of OSINT in investigations carried out by both federal and state public prosecutors.[81]

IV.2.b. Military Police

The Military Police have also carried out social media surveillance using OSINT techniques. This is evidenced by the case of João Reginaldo da Silva Júnior,24, from Uberlândia. During a visit to his city by then-President Jair Bolsonaro, he wrote on his Twitter account: "Guys, Bolsonaro in Udia tomorrow... Anyone looking to become a

[81] Asociación para el Progreso de las Comunicaciones, Article 19 Brazil and South America, Derechos Digitales e Intervozes, UN Human Rights Council's Universal Periodic Review, 41st Session, "Contribución conjunta de las partes interesadas," 2022, § 28, retrieved from:
https://www.apc.org/sites/default/files/upr_brazil-sp-final.pdf, last access: August 14, 2023.

national hero?" João was arrested after the Military Police classified his post as "propaganda and incitement to commit crimes against the physical integrity and life of the President of the Republic Jair Messias Bolsonaro, with suggestions that such threats would be carried out during his visit to this city of Uberlândia today."[82] Although he was released a few hours later,[83] the judicial case against him proceeded. According to press reports, the Federal Public Prosecutor's Office (MPF) offered a plea deal (or transação penal) to João and six others who had posted messages about Bolsonaro on Twitter during his visit to Uberlândia. The deal included a fine of twenty thousand reais (R$20,000) for each individual involved, which, if accepted, would prevent further prosecution. João's lawyers stated they would reject the offer.[84]

IV.2.c. Ministry of Defense

The Ministry of Defense reported that it had found contracts in its records with third parties that provide OSINT services. Among others, it referred to Contract 01/2021, signed with the company Supernova Serviços de Informação LTDA, for "providing social media monitoring services." The terms of the contract specify that it involves permanent monitoring ("24x7") for one year of "the agency's image on social media, including blogs," and that "the results of this activity must indicate impact (what), influential profiles (who), media (where, when), reputation and polarization (how), trends, the Brazilian context, and other strategic information relevant for decision-making, such as negative engagement."[85]

---

[82] Rodrigues, Fabiano, "Jovem é preso em flagrante após publicação sobre visita de Bolsonaro a Uberlândia," G1 Triângulo e Alto Paranaíba, 2021, retrieved from: https://g1.globo.com/mg/triangulo-mineiro/noticia/2021/03/04/jovem-e-pre-so-apos-publicacao-sobre-vinda-de-bolsonaro-a-uberlandia.ghtml, last access: August 14, 2023.

[83] Ibid.

[84] Borge, Luis Fellipe, "MPF propõe multa de R$ 20 mil a jovem detido por publicação sobre visita de Bolsonaro em MG," G1 Triângulo e Alto Paranaíba, 2023, retrieved from: https://g1.globo.com/mg/triangulo-mineiro/noticia/2023/02/03/mpf-propoe-multa-de-r-20-mil-a-jovem-detido-por-publicacao-sobre-visita-de-bolsonaro-em-mg.ghtml, last access: August 14, 2023.

[85] It can be downloaded from Government of Brazil, Ministry of Defense, "Contratos formalizados na administração central do Ministério da Defesa (ACMD)," 2019, retrieved from: https://www.gov.br/defesa/pt-br/acesso-a-informacao/lici-tacoes-e-contratos-1/contratos-vigentes-na-administracao-central-do-ministerio-da-defesa-acmd-1/contratos-formaliza-dos-na-administracao-central-do-ministerio-da-defesa-acmd, last access: August 14, 2023.

IV.2.d. Office of the President

Reports indicate that the Office of Presidential Communications signed a contract with a private company to profile 77 journalists and social media influencers. The targeted individuals were classified into three groups based on the tone of their posts toward the government: "favorable," "neutral/informative," and "detractor." This "influencer map" also included recommendations regarding "actions to follow" in relation to each profiled individual.[86] The document further contained the phone numbers and email addresses of the individuals under observation.[87]

IV.2.e. Ministry of Justice

The Ministry of Justice reported that it does not conduct OSINT. However, we should highlight the case of the so-called "anti-fascist dossier." The dossier was a confidential document produced by the Secretariat for Integrated Operations (SEOPI) of the Ministry of Justice, which mapped and surveilled 579 federal and state officials from various sectors of security, the state bureaucracy, and universities, who were identified as members of the "anti-fascist movement."[88] In addition to information on the officials, the dossier included a range of data gathered from open sources, such as names, addresses, photographs, social media URLs, and other personal details. The document circulated among public security and intelligence agencies.

A similar document, drafted by Douglas Garcia, a state legislator from São Paulo, containing personal information and data on over one thousand individuals labeled as "terrorists," was reportedly handed over to the U.S. government by Eduardo

---

[86] Valente, Rubens, "Relatório do governo separa em grupos jornalistas e influenciadores," UOL, 2020, retrieved from: https://noticias.uol.com.br/colunas/rubens-valente/2020/12/01/governo-bolsonaro-jornalistas-redes-sociais.htm, last access: August 14, 2023.

[87] Valente, Rubens, "Veja a lista de jornalistas e influenciadores em relatório do governo," UOL, 2020, https://noticias.uol.com.br/colunas/rubens-valente/2020/12/01/lista-monitoramento-redes-sociais-governo-bolsonaro.htm, last access: August 14, 2023.

[88] Valente, Rubens, "Ação sigilosa do governo mira professores e policiais antifascistas," UOL, 2020, retrieved from: https://noticias.uol.com.br/colunas/rubens-valente/2020/07/24/ministerio-justica-governo-bolsonaro-antifascistas.htm, last access: August 14, 2023. Observatorio Legislativo CELE, newsletter of June, 2022, retrieved from: https://observatoriolegislativocele.com/boletin-mensual-observatorio-legislativo-junio-2022, last access: August 14, 2023.

Bolsonaro, federal legislator and son of the former president.[89] On August 19, 2020, the Supreme Federal Court of Brazil suspended the creation of the dossier, and in May 2022, the full court declared it unconstitutional.[90]

Regarding software acquisition for OSINT, on May 19, 2021, the Ministry of Justice issued Tender Notice No. 03/2021 for the operational needs of the Intelligence Directorate of SEOPI. The objective of the tender was "the acquisition of an open-source intelligence solution, including social media, the deep web, and the dark web, covering supply, installation, and configuration, as well as technical support, in response to the operational needs of the Intelligence Directorate of the Secretariat for Integrated Operations (DINT/SEOPI)." The winning bidder was Harpia Tech. According to the information provided by the company during the bidding process, "the program offered by the company monitors 5,722 sources, spread across 112 countries." The proposal explained that "a source is understood to be: a social network, a channel in a messaging group, a forum in the dark web, etc." and that among the sources the program monitors are those "reflecting the following phenomena: hacktivism, cybercrime, academic publications, exploits, scripts, attack tools, cyber espionage, open data published by security companies, media groups, and research institutions."[91] In 2021, a coalition of civil society organizations obtained a precautionary measure that halted the Ministry of Justice's procurement process with this company, but in 2022, the Federal Court of Accounts lifted the measure and authorized the contract.[92]

---

[89] Carta Capital, "Eduardo Bolsonaro entregou dossiê de antifascistas aos EUA, diz deputado à Justiça," 2020, retrieved from:
https://www.cartacapital.com.br/politica/eduardo-bolsonaro-entregou-dossie-de-antifascistas-aos-eua-diz-deputado-a-justica, last access: August 14, 2023.

[90] Find the content of the judgment in the Supreme Federal Court, "Rede Sustentabilidade c. Bruno Lunardi Goncalves y otros," 2020, retrieved from: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5967354, last access: August 14, 2023.

[91] Zanatta, Rafael A., "O que sabemos sobre o Harpia Tech?" Data Privacy BR, 2022, retrieved from:
https://www.datapriva-cybr.org/o-que-sabemos-sobre-a-harpia-tech, last access: August 14, 2023.

[92] Hirabahasi, Gabriel, "TCU libera contrato do Ministério da Justiça para sistema de inteligência," CNN Brasil, 2022, retrieved from:
https://www.cnnbrasil.com.br/nacional/tcu-libera-contrato-do-ministerio-da-justica-para-uso-de-sistema-espiao-pegasus, last access: August 14, 2023.

IV.3. Colombia

From the terms of Resolution No. 5,839/2015 of the National Police, it follows that only the National Police's Virtual Cyber Center is authorized to conduct "cyber-patrolling" and "to identify threats originating from or directed toward Colombia that affect citizen cybersecurity, developing the capacity to identify and detect common factors in known incidents, as well as breaches of the availability, integrity, and confidentiality of the information circulating in cyberspace." However, under the protection of the aforementioned regulation, OSINT activities are being carried out in contexts other than those authorized by the rule (cybercrime investigations)[93] and even by entities other than the National Police.

IV.3.a. Attorney General's Office

The Office of the Attorney General of the Nation informed this investigation that, although it does not have a unit specifically tasked with this role, it does conduct open-source consultations within the framework of Article 244 of the Code of Criminal Procedure, which establishes that: "The Judicial Police, in the course of their investigative activity, may conduct comparisons of data recorded in mechanical, magnetic, or similar databases, provided that it involves the simple comparison of publicly accessible information."

IV.3.b. National Police

The responses to the public information requests submitted as part of this investigation show that the National Police has signed "contracts with entities that provide services for conducting cyber-patrolling activities on open sources."

In addition, according to responses to public information requests submitted by the Fundación para la Libertad de Prensa (FLIP) [Foundation for Press Freedom] and Fundación Karisma, "cyber-patrolling activities include the consultation, observation, and collection of online information from open and public data and content on the

---

[93] This contradicts the stance of the Inter-American Commission on Human Rights' Special Rapporteur for Freedom of Expression, which recommends limiting the scope of 'cybersecurity' to criminal acts that directly threaten the integrity of networks and internet infrastructure—not broader offenses. See IACHR, "Libertad de expresión e internet," report by the Special Rapporteur for Freedom of Expression, OEA/Ser.L/V/II, CIDH/RELE/INF.11/13, December 31, 2013, §§ 118 and 119, retrieved from: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf, last access: August 14, 2023.

internet and social media."[94] Furthermore, in a public statement in 2021, former Police Director Jorge Luis Vargas addressed the issue, describing cyber patrolling as being akin to ordinary patrols but conducted on the internet, and that "in that public space, where the law allows it, the authorities must perform this surveillance service."[95]

During the 2021 national strike, it was reported that Colombian authorities were conducting mass internet monitoring aimed at identifying "allegedly false content about the development of the protests, efforts to discredit the image of public security forces, as well as incitement to public hatred. These measures were intended to determine which information was false or true and, in this way, to combat alleged "digital terrorism" actions that could potentially exacerbate violence."[96] The Colombian State informed the Inter-American Commission on Human Rights (IACHR) that, within this framework, 21,675 hours of cyber-patrolling were carried out, and at least 154 fake news stories and more than 2,300 posts containing threats to someone's life or physical integrity were identified.[97] Also, during the national strike, the police collected information on protesters by monitoring their social media. This monitoring led to the identification and arrest of several individuals.[98]

For all these reasons, the IACHR issued a recommendation to the Government to "cease police activities aimed at categorizing content as 'false' or 'true' and to refrain

---

[94] Camacho Gutiérrez, Lucía, Ospina Celis, Daniel and Upegui Mejía, Juan Carlos, Inteligencia estatal en internet y redes sociales: el caso colombiano, Bogota, Dejusticia, 2022, p. 31, retrieved from: https://www.dejusticia.org/wp-content/uploads/2022/12/InteligenciaEstatalEnInternet-Web-Dic23.pdf, last access: August 14, 2023.

[95] Revista Semana, "¿Qué es el ciberpatrullaje?" 2021, retrieved from: https://ne-np.facebook.com/RevistaSemana/videos/qu%C3%A9-es-el-ciberpatrullaje/438397297775230/? so =permalink& rv =related_videos, last access: August 14, 2023.

[96] IACHR, Organization of the American States (OAS), "Visita de trabajo a Colombia: observaciones y recomendaciones. Visita: junio 2021," 2021, § 176, retrieved from: https://www.oas.org/es/cidh/informes/pdfs/ObservacionesVisita_cidh_Co-lombia_spA.pdf, last access: August 14, 2023.

[97] Report from the State to the IACHR, June 8, 2021, p. 64, cited in CIDH-OEA, (n. 94, § 176).

[98] Fundación Karisma, "Sobre la estigmatización a integrantes de la 'primera línea' y a creadores de contenido," 2022, retrieved from: https://web.karisma.org.co/sobre-las-recientes-capturas-a-integrantes-de-la-primera-linea-y-a-creadores-de-contenido, last access: August 14, 2023.

from assigning stigmatizing labels or criminalizing those who express themselves on the internet about the protests."[99]

IV.3.c. Colombian Army

In 2020, the press revealed that the Army had carried out a digital surveillance program targeting more than 130 intelligence objectives, including politicians, union leaders, and civil society organizations. As part of that program, "using computer tools and software, they conducted searches and massively and indiscriminately collected all possible information on their targets to prepare military intelligence reports. Telephone numbers, home and work addresses, email accounts, friends, relatives, children, and colleagues' contacts, traffic violations, and even voting locations were part of these profiles."[100] Some Army officials reportedly attempted to justify this conduct by claiming that the information had been collected from open sources.

Also in 2020, the National Army compiled a list of users[101] on its official Twitter account (@col_ejercito), which it titled "Opposition," and which included 33 accounts belonging to media outlets, journalists, social organizations, political activists and leaders (including, for example, Gustavo Petro), human rights activists, international organizations (among them, the account of the Office of the United Nations High Commissioner for Human Rights), and even the account of the Special Jurisdiction for Peace of Colombia. After the situation became public, the Army issued a statement calling it a mistaken decision and deleted (or hid) the list.[102]

---

[99] Report from the State to the IACHR, June 8, 2021, p. 64, cited in CIDH-OEA, (n. 94, Recommendation No. 40).

[100] Revista Semana, "Las carpetas secretas," 2020, retrieved from: https://www.semana.com/nacion/articulo/espionaje-del-ejercito-nacional-las-carpetas-secretas-investigacion-semana/667616, last access: August 14, 2023.

[101] For more information on the list of users, see Centro de Ayuda Twitter, "Cómo usar las listas de Twitter," retrieved from: https:// help.twitter.com/es/using-twitter/twitter-lists, last access: August 14, 2023.

[102] See https://twitter.com/cuestion_p/status/1237382254952763392, last access: August 14, 2023, and https://twitter.com/flip_org/status/1237499772069711874, last access: August 14, 2023.

IV.3.d. Detecting Fake News During the Pandemic

In 2020, the Puesto de Mando Unificado de Ciberseguridad [Unified Cybersecurity Command Post][103] monitored internet activity in search of "fake news." In response to a public information request submitted by FLIP,[104] that body stated that "it identifies fake news based on information published in open sources." Between March 30 and April 26 of that year, the National Police published daily reports on the fake news it had identified online.[105]

IV.3.e. Office of the President

In 202 0, the Foundation for Press Freedom (FLIP) published a report warning that the Office of the President had allegedly contracted the marketing firm Du Brands to monitor more than 450 social media influencer accounts. Each of them was profiled as "positive," "neutral," or "negative" based on whether their content aligned with or opposed the Government's political positions.[106] One of the profiled individuals filed a tutela action (a writ for the protection of constitutional rights) against the Government, claiming that the creation of the list had violated their right to habeas data. The case reached the Supreme Court, which ruled in favor of the plaintiff, holding that their inclusion—without prior consent, in a list based on a sensitive data point such as political affiliation—violated their fundamental right to habeas data, regardless of whether the data had been made public by the claimant.[107]

---

[103] The Puesto de Mando Unificado de Ciberseguridad was composed of the Office of the President (CSIRT Presidencia), the Ministry of Defense (COLCERT), the Ministry of Information and Communication Technologies (MINTIC), the Attorney General's Office, the Armed Forces (CCOCI), the National Police, and the National Intelligence Directorate.

[104] National Ministry of Defense, National Police, Directorate of Criminal Investigation and Interpol, No. GS-2021, DIJIN-CE- CIP-1.10, 2021, retrieved from: https://drive.google.com/file/d/1Z7AKesIM_LY5Jde8tH2mQnDbyNZCc2a-/view, last access: August 14, 2023.

[105] Reports in the Republic of Colombia, National Police, "Reporte de noticias falsas detectadas por CAI virtual," 2020, retrieved from: https://www.policia.gov.co/reporte-fakenews, last access: August 14, 2023.

[106] El Espectador, "La lista de influenciadores a los que la Presidencia les pone el ojo," 2020, retrieved from: https://www.elespectador.com/politica/la-lista-de-influenciadores-a-los-que-la-presidencia-les-pone-el-ojo-articl e, last access: August 14, 2023. Revista Semana, "Positivo, negativo, neutro: lista de influenciadores perfilados por el Gobierno," 2020, retrieved from: https://www.semana.com/nacion/articulo/positivo-negativo-neutro-lista-de-influenciadores-perfilados-por-el-g obierno/697304, last access: August 14, 2023.

[107] Republic of Colombia, Supreme Court of Justice, judgment No. STP9319-2020, October 27, 2020, Court of Criminal Appeals, Tutelage Decision Chamber No. 1, retrieved from: https://cortesuprema.gov.co/corte/index.php/2021/02/22/derecho-al-habeas-data, last access: August 14, 2023.

IV.4. Mexico

In the absence of detailed and transparent public information regarding the use of open-source intelligence, information access requests were submitted to the Secretariat of Security and Citizen Protection (SSPC), the National Guard (GN), and the Executive Secretariat of the National Public Security System (SESNSP). The cited agencies responded that they do not have relevant data regarding practices for collecting data and information through open sources, nor do they have contracts with private companies for conducting OSINT. However, it has been confirmed that at least the following state agencies have used OSINT for surveillance purposes.

IV.4.a. National Intelligence Center

The Multi-Source System of the National Intelligence Center (CNI) allows the analytical units of public security institutions to integrate information effectively and efficiently.[108] This does not preclude the system from using information available on social media to "understand the behavior of individuals and the social structures formed within communities" and to detect "criminal and antisocial behavior" through the "constant monitoring of social media," so that authorities can "anticipate potential criminal acts that may endanger public safety" and "implement preventive actions to avoid the escalation of detected risks."[109] The system is also used to "analyze networks of connections between actors or agents relevant to an investigation."[110]

A source close to the CNI, interviewed for this investigation, explained that the organization defines open sources as "publicly available content such as social media posts—including videos or eyewitness accounts of events. Essentially, it is public information posted on social media by someone." They also reported that the system does not include specific protocols to regulate or limit OSINT practices.[111]

---

[108] Modelo Nacional de Policía y Justicia Cívica, "Sistema multi-fuente para la estimación de la incidencia delictiva orientada a la inteligencia policial," 2020, p. 15, retrieved from: https://www.gob.mx/cms/uploads/attachment/file/590581/sistema_multi-fuente_PP.pdf, last access: August 14, 2023.

[109] Ibid., p. 28.

[110] Ibid., p. 28.

[111] Article 19, interview with CNI collaborator, October 20, 2022.

Additionally, a news report[112] revealed that one of the Regional Intelligence Fusion Centers (CERFI), located in the 27th Infantry Battalion in Iguala, Guerrero, carries out monitoring activities, including the interception of private communications. The report also states that the CERFI performs call interception, geolocation, access to social networks, and data retrieval. It further highlights the use of a comprehensive intelligence platform that includes an OSINT module, which collects data from social media platforms.

IV.4.b. National Guard

According to the 2021 National Federal Public Security Census, in 2020, the Scientific Division of the National Guard, through "cyber monitoring," identified and deactivated 5,920 websites involved in illegal activities, including 342 sites related to financial and personal data theft.[113] Additionally, on October 3, 2022, the National Guard issued Call for Bids IA-036H00998-E267-2022, for the hiring of a "training service to deliver a course on Open Source Intelligence (OSINT),"[114] which would cover the following topics: i) intelligence theory and methodological concepts; and ii) tools and databases. The course was tentatively scheduled to be held in Mexico City during November and December 2022. The existence of this call, which was later removed from the official website, contradicts the National Guard's response to the information access request submitted for this investigation, in which the agency claimed that there was no information regarding OSINT practices.

---

[112] Ocampo Torres, Lenin, "En Iguala funciona un centro regional de espionaje del Ejército, revela el hackeo del grupo Guacamaya," El Sur, 2022, retrieved from: https://suracapulco.mx/en-iguala-funciona-un-centro-regional-de-espionaje-del-ejercito-revela-el-hackeo-del-grupo-guacamaya, last access: August 14, 2023.

[113] Instituto Nacional de Estadística y Geografía (INEGI), "Censo Nacional de Seguridad Pública Federal. Presentación de resultados generales," 2021, updated April 11, 2022, retrieved from: https://www.inegi.org.mx/contenidos/programas/cnspf/2021/doc/cnspf_2021_resultados.pdf, last access: August 14, 2023.

[114] The call for bids was removed from the portal, although the document (PDF) is still available from the Secretariat of National Defense (SEDENA) and the National Guard (GN), "Convocatoria para la invitación nacional a cuando menos tres personas, electrónica," 2022, retrieved from: https://www.gob.mx/cms/uploads/attachment/file/765949/Convocatoria_IA-E267-2022_Curso_de_Inteligencia_en_Fuentes_Abiertas.pdf, last access: August 14, 2023.

IV.4.c. Federal Entities

It has come to light that the states of Guerrero, Chihuahua, and Veracruz have acquired software related to OSINT. The Executive Secretariat of the State Public Security System of Guerrero recorded the purchases of OSINT-related software between January and June of 2021 and 2022, with an allocated budget of MXN 387,000 (USD 19,903.41). The software was intended for "searching for sensitive information and conducting investigations through OSINT."[115]

The state of Chihuahua published the document "Evaluación del Programa para el Fortalecimiento del Estado de Fuerza y las Capacidades Institucionales" [Evaluation of the Program for Strengthening Institutional Capabilities and the State Force][116] in October 2020, which outlined the creation of a cyber police force equipped with advanced technology for cyber patrolling. It also noted that personnel involved in these activities possess specialized OSINT technical knowledge to gather information from various websites, blogs, social media, and other virtual media.[117] The data obtained during cyber patrolling is processed and analyzed to generate "intelligence reports identifying fake profiles with specific modus operandi or unusual activities that may threaten cybersecurity."[118] In response to these findings, a public information request was submitted to the State Public Security Secretariat of Chihuahua, with no response.

In turn, the 2021 State Evaluation Report for the state of Veracruz indicates that the state acquired and renewed specialized software licenses for tasks carried out by the

---

[115] Information regarding the software is available in the open data of the National Transparency Platform, under the term "OSINT", retrieved from: https://buscador.plataformadetransparencia.org.mx/web/guest/buscadornacional?buscador=OSINT&coleccion=5, last access: August 14, 2023.

[116] Government of the State of Chihuahua, "Evaluación del Programa para el Fortalecimiento del Estado de Fuerza y las Capacidades Institucionales," 2020, retrieved from: https://www.gob.mx/cms/uploads/attachment/file/604448/DIAGNO_STI-CO_CHIHUAHUA_2020.pdf, last access: August 14, 2023.

[117] Ibid.

[118] Ibid., p. 11.

Preventive Scientific Police — including OSINT—[119] with the objective of "strengthening and improving the performance of the Scientific Police and combating cybercrime." In response to an information access request made as part of this investigation, the State Public Security Secretariat reported that "open-source intelligence is defined as the search for public information on the internet, as established in Article 143[120] of Law No. 875 on Transparency and Access to Public Information for the state of Veracruz." It is worth noting that this law defines public information as that "held by obligated subjects, except for information that is classified as confidential or restricted,"[121] that is, in the sense commonly used in transparency laws, and not in reference to its level of access.

IV.5. Uruguay

IV.5.a. National Computer Security Incident Response Center

From the responses to public information requests submitted as part of this investigation, it appears that the Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTUY) [National Computer Security Incident Response Center] contracted a Threat Intelligence license from the company ITSEC S.A. in 2020 for USD 170,800. The contract was awarded through a public bidding process[122] and took place within the framework of the Cybersecurity Strengthening Program in Uruguay, signed in 2019 with the Inter-American Development Bank (IDB), to improve the prevention, detection, and response to cyberattacks.

---

[119] Government of the State of Veracruz, State Public Security Secretariat (SSP) and the Executive Secretariat of the State Public Security System and Council (SESCESP), "Evaluación integral del fondo de aportaciones para la Seguridad Pública (FASP) del estado de Veracruz, ejercicio fiscal 2021," state evaluation report, 2021, retrieved from:
http://ftp2.fiscaliaveracruz.gob.mx/WEB%20FGE/FASP/2021/Evaluacion-Integral-FASP-Veracruz-2021.pdf, last access: August 14, 2023.

[120] Congress of the State of Veracruz, General Secretariat, Directorate of Legislative Registry and Official Publications, "Ley de Transparencia y Acceso a la Información pública para el estado de Veracruz de Ignacio de la Llave," 2022, retrieved from:
https://www.legisver.gob.mx/leyes/LeyesPDF/LTRANSPARENCIA20122022.pdf, last access: August 15, 2023.

[121] Ibid.

[122] Government of Uruguay, State Procurement Regulatory Agency, "PFI - Licitación pública nacional 3/2020," 2020, retrieved from: https://www.comprasestatales.gub.uy/consultas/detalle/id/818602/mostrar-llamado/1, last access: August 14, 2023.

The bidding call reveals the characteristics of the system. It specified, among other requirements, that the system must include "access to multiple threat information sources, at a minimum: social media, hacker message boards and forums, IRC, paste sites, blogs, and dark webs." It must also have "access to social media posts, including at least: Twitter, Facebook, and Reddit." Additionally, it had to "provide access to special-access forums (Onion pages) on the dark web," among other features.[123]

IV.5.b. Public Prosecutor's Office

An interview conducted with a qualified source from the Attorney General's Office confirmed that, in the context of criminal investigations, information is collected on identified individuals, and that the undercover agent provision could be used to create fake profiles. Additionally, the source noted that there are no protocols for collecting and processing information gathered from open sources.[124]

The qualified informant from the Prosecutor's Office emphasized that, at present, there are no sufficient safeguards regarding the use of OSINT by the police in Uruguay. They also pointed out additional concerns, such as police corruption and lack of training among police officers (and even within the Attorney General's Office) in handling information. They further noted that cases of information leaks or misuse of police system data for private purposes are publicly known.[125]

IV.5.c. Ministry of the Interior

Several months after the deadline for responding had expired, and following a complaint filed with the Public Information Access Unit of Uruguay, the Ministry of the Interior classified the information requested for this investigation regarding the use of OSINT techniques and the existence of protocols for its use. It applied information

---

[123] Presidency of Uruguay, Agency for Electronic Government and Information and Knowledge Society (AGESIC), "Documentos de licitación para adquisición de licencia de Threat Intelligence," 2020, retrieved from: https://docs.google.com/document/d/1Ygz2fYqqqcS3QKX6i5Sh_gvwa68Yi5CuUUvWxbJXBKg/edit, last access: August 14, 2023.

[124] Interview conducted on December 6, 2022.

[125] See Diario Ámbito, "Caso Astesiano: los chats del ex custodio que complican a policías y funcionarios," 2022, retrieved from:
https://www.ambito.com/uruguay/caso-astesiano-los-chats-del-ex-custodio-que-complican-policias-y-funcionari-os-n5603158, last access: August 14, 2023.

classification criteria that the Public Information Access Unit has already deemed illegal in its rulings.[126]

In its 2020 Annual Report,[127] the Ministry of the Interior stated that the National Observatory on Violence and Crime "has recently incorporated social network analysis software (UCINET) into its set of IT tools, which will allow for a deeper examination of the relational aspects of criminality—an essential feature that has not yet been addressed in our country with the importance it deserves." UCINET is a specialized software tool that supports OSINT efforts by enabling the analysis and visualization of social networks. It offers an extensive suite of statistical measures and indicators, leveraging relationship matrices to examine connections between individuals or entities. "Social network analysis" is used broadly and does not necessarily refer to digital social networks (such as Twitter, Facebook, or Instagram). Instead, it applies to the detection of patterns and relationships between individuals in any type of network. When asked about the purpose and protocols for using this software, the Ministry of the Interior of Uruguay classified the information as restricted.

IV.5.d. Access to Information Request on Cyber-Patrolling

In June 2020, the local newspaper Salto al Día reported that, according to a source from the Cybercrime Unit of the Uruguayan Police, around 200,000 individuals had allegedly been identified for participating in social media groups, mainly with left-wing political affiliations.[128] Gustavo Gómez, director of the human rights organization Observacom, submitted a public information request to determine

---

[126] See Presidency of Uruguay, AGESIC, Public Information Access Unit (UAIP), "Dictamen Nº 17/013 sobre información reservada y matrices de criterios," 2013, retrieved from: https://www.gub.uy/unidad-acceso-informacion-publica/institucional/normativa/dictamen-n-17013-sobre-informacion-reservada-matrices-criterios, last access: August 14, 2023. See Presidency of Uruguay, AGESIC, UAIP, "Consejo Ejecutivo de la Unidad de Acceso a la Información Pública," Resolution No. 13/22, 2022, retrieved from: https://www.gub.uy/unidad-acceso-informacion-publica/sites/unidad-acceso-informacion-publica/files/2022-06/RESUAIP22013-%20AA%20con%20MI.pdf, last access: August 14, 2023.

[127] Presidency of Uruguay, "Memoria anual 2020," volume II, retrieved from: https://medios.presidencia.gub.uy/tav_portal/2021/noticias/AH_438/Tomo%20II_FINAL%20web.pdf, last access: August 14, 2023.

[128] Salto al Día, "Delitos Informáticos tendría identificado a más de 200 mil personas por expresiones de odio en redes sociales," 2020, retrieved from: https://web.archive.org/web/20200811033653/https://saltoaldia.com.uy/delitos-informaticos-tendria-identificado-a-mas-de-200-mil-personas-por-expresiones-de-odio-en-redes-sociales, last access: August 14, 2023.

whether “the Uruguayan police systematically monitor social media to identify hate speech.”[129] In response, the Ministry of the Interior rejected the petition, stating that "the requested information is classified as 'restricted'."[130]

V. OSINT and Human Rights

V.1. Impact on Privacy

Privacy is a right constitutionally guaranteed in many countries of the region (Argentina, Bolivia, Brazil, Chile, Colombia, Mexico, Uruguay, and Venezuela, among others) and its protection is provided for both in the Universal Human Rights Protection System (UHRPS) and in the Inter-American Human Rights Protection System (IAHRPS). The fact that the “right to privacy” is not explicitly mentioned in these instruments does not mean that it is not a fundamental human right enshrined in the treaties.[131]

At the universal level, Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) prescribe that no one shall be subjected to arbitrary interference with their privacy, family, home or correspondence, nor to attacks on their honor or reputation. Regionally, the relevant article on the protection of honor and dignity is Article 11 of the American Convention on Human Rights (ACHR). The Inter-American Court of Human Rights (hereinafter, I/A Court H.R.) has stated that the privacy referred to in this article includes, among other dimensions, the right to freely make decisions related to various aspects of one's life, having personal space for peace, keeping certain aspects of private life confidential and controlling the dissemination of personal information to the public.[132] However, the rights included in Article 11 are not absolute and are subject to the application of the proportionality test.[133]

---

[129] See https://twitter.com/gusgomezgermano/status/1311650905134166017, last access: August 14, 2023.
[130] See https://mobile.twitter.com/gusgomezgermano/status/1311650940458536960, last access: August 14, 2023.
[131] Bertoni, (n. 21.)
[132] Inter-American Court of Human Rights (I/A Court H.R.), “Fontevecchia y D’amico vs. Argentina,” judgment of November 29, 2011, Merits, Reparations, and Costs, Series C, No. 238, § 48, retrieved from: https://www.corteidh.or.cr/CF/jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=191, last access: August 14, 2023.
[133] Bertoni, (n. 21.)

> The right to privacy is not an absolute right and, therefore, may be restricted by States provided that such interferences are not abusive or arbitrary; thus, they must be established by law, pursue a legitimate aim, and meet the requirements of suitability, necessity, and [strict] proportionality, that is, they must be necessary in a democratic society.[134]

Regarding the relationship between privacy and communications, the I/A Court H.R. stated "although telephone conversations are not explicitly mentioned in Article 11 of the Convention, they are nevertheless a form of communication that, like correspondence, falls within the scope of protection of the right to privacy."[135] It is important to emphasize that, for the Inter-American Court of Human Rights (I/A Court H.R.), violations of privacy can originate from both the State and private actors.[136]

Likewise, in the case "Pavez Pavez v. Chile," the Inter-American Court of Human Rights (I/A Court H.R.) interpreted the concept of "private life" broadly, establishing that its protection "is not limited to the right to privacy, since it encompasses a series of factors related to the dignity of the individual, including, for example, the capacity to develop his or her own personality and aspirations, determine his or her identity and define his or her personal relationships."[137] For its part, the European Court of

---

[134] I/A Court H.R., "Tristán Donoso vs. Panamá," judgment of January 27, 2009, Preliminary Objections, Merits, Reparations, and Costs, Series C, No. 193, § 56, retrieved from: https://www.corteidh.or.cr/CF/jurisprudencia2/ficha_tecnica.cfm?nId_Fi- cha=253, last access: August 14, 2023.

[135] Ibid., § 55, cited in Bertoni, (n. 21).

[136] Bertoni, (n. 21.)

[137] "58. At the same time, the Court has specified that the protection of the right to private life is not limited to the right to privacy since it encompasses a series of factors related to the dignity of the individual, including, for example, the capacity to develop his or her own personality and aspirations, determine his or her identity and define his or her personal relationships. The concept of privacy also covers aspects of physical and social identity, including the right to personal autonomy and personal development, and the right to establish and develop relationships with other human beings and with the outside world. The effective realization of the right to private life is decisive for the possibility of exercising personal autonomy in relation to the future course of events that are relevant to an individual's quality of life. Furthermore, private life encompasses the way in which individuals see themselves and how they decide to project themselves towards others, this being an essential condition for the free development of the personality." I/A Court H.R., "Pavez Pavez vs. Chile," judgment of February 4, 2022, Merits, Reparations, and Costs, retrieved from: https://www.corteidh.or.cr/docs/casos/articulos/seriec_449_esp.pdf, last access: August 14, 2023.

Human Rights (ECHR) in the case "Peck v. United Kingdom"[138] acknowledged that there is an expectation of privacy even when people interact in public spaces.[139] These expansive and generous interpretations of the right to privacy lead us to consider the possibility that it may even extend to public posts on social media, whose reach can be restricted by users—even in cases where, for any reason, they have not done so."

By definition, OSINT uses "open" sources but can still violate the right to privacy. The legal definition of "open source" will be fundamental in determining this.

Online open sources are typically defined as information "publicly accessible" or "available to the general public." However, this is not without problems. "Public access" is a nebulous concept. In the context of online activity, it may refer to the fact that the user uploading the content has chosen not to limit its visibility exclusively to their contacts. In this sense, a publication could be considered "open to the public." However, this assertion can—and should—be nuanced. To access a specific post, one must enter a platform, either through an app or by typing a URL into a web browser, and then, within the platform, locate a specific user's profile page or find the thread in which the post was made. The ability to post content in a way that is reserved for certain people is not a feature available on every platform, nor is it one that all users are familiar with or regularly implement.

Not all published material is publicly accessible. Many platforms restrict content, requiring user authentication, such as account registration or login credentials, before granting access. In such cases, the content is not accessible to the general public but only to those with accounts, sometimes a paid one. This is the case for many academic publications and even media outlets or journalistic archives. In other words, not all published material is accessible or unrestricted.[140] Finally, in the case of social media, even if a person sets their profile posts to remain private, they may not have control over the visibility of their interactions on posts on third-party profiles (for example,

---

[138] See European Court of Human Rights, "Peck v. The United Kingdom," judgment of January 28, 2003, retrieved from:
https://hudoc.echr.coe.int/fre#{%22fulltext%22:[%22peck%22],%22itemid%22:[%22001-60898%22]}, last access: August 14, 2023.

[139] Bertoni, (n. 21.)

[140] Media outlets like Clarín (Argentina), Folha de S. Paulo (Brazil), El Mercurio (Chile), El Espectador (Colombia), Reforma (México)

comments on other people's photographs), and they might not even know whether the profile they are interacting with is "publicly accessible" or private.[141]

Another issue with the concept of an open source is that it "does not depend on how many people have actually accessed or are aware of its existence but rather on how hypothetically difficult it would be for a person to access certain information (...). It is pure conjecture."[142] This hypothetical exercise equates situations that, in reality, are not the same: a tweet from a world-famous athlete, a TV star, or a head of state is considered as "public" as a family photo blog created for a specific occasion. The various legislations reviewed do not take this into account when defining "open sources."

The rules that clearly distinguish between information available in "open sources" and other types are based on the same premise: if the data is "publicly accessible," its holder has no expectation of privacy regarding the state. In the case of the internet, this implies assuming that, by choosing to make their interactions "public" in the sense outlined previously, the user has waived their expectation of privacy.[143] However, this is not necessarily so. When publishing content online, individuals do not anticipate that such content will be subjected to state scrutiny. This is especially true when there are no specific regulations authorizing such practices. Unlike individuals, state action is limited to the scope of its legal competence, that is, to those powers granted by the legal system. Moreover, constitutional rights cannot be overridden by the terms and conditions of online platforms or by the architecture of the internet.

As we have seen, there is a tendency to group all kinds of information under the categories of "open source" or "public access." The only common denominator is that these are sources of relatively "easy" access. There is not even a consistent distinction between information a person has freely published about themselves and information about them available online, published by someone else, with or without their consent.

---

[141] This is the case, for example, of comments on third-party profiles on Facebook and Instagram.

[142] Hartzog, Woodrow, "The Public Information Fallacy," in: Boston University Law Review, vol. 99, No. 459, 2019, p. 498.

[143] Kerr, Orin S., "Applying the Fourth Amendment to the Internet: A General Approach," in: Stanford Law Review, vol. 62, No. 1,005, 2009, p. 1,030-1,031.

This perspective suggests a 'digital public space' concept, equating the open internet—or at least its publicly accessible portion—to physical public spaces like parks or streets. If the internet's publicly accessible content is functionally equivalent to a public street, this logic permits governments to conduct preventive "patrols" without judicial oversight—justified as necessary for public safety. However, this premise is wrong. The internet is not the functional equivalent of a public street. The state's authority to monitor public streets for safety purposes derives from its role as custodian of public spaces. This status not only ensures free access but also establishes state ownership, from which the duty to ensure the safety of those who use them arises. This explains why police cannot routinely patrol private spaces like museums or shopping centers, even when open to the public, as these remain under third-party ownership. The public's expectation of privacy from the state within such establishments is greater than on a public street. Interactions between customers in a shopping center should not be monitored by Security Forces outside the framework of an investigation and without a court order. Similarly, the fact that it is "relatively easy" to access the content of online posts (as long as there is a URL) does not mean that monitoring them without a court order does not constitute an infringement upon the right to privacy.

Even if this mistaken framing of the digital public space was accepted, "patrolling" the internet differs significantly from the actions of Security Forces patrolling public streets. First, modern web scraping tools enable rapid, large-scale data extraction at a fraction of the cost of manual collection. The use of such programs is far more invasive than street patrolling, as it collects much more information than is strictly necessary for the intended state purposes. Therefore, the use of scrapers could fail to meet the standards of necessity and proportionality required by International Human Rights Law.[144] A conception of the internet as a digital public space compatible with the rule of law must recognize it as a valuable civic space, where rights are fully upheld and which must be protected from undue interference.

Furthermore, the so-called "cyber patrolling" is conducted secretly, and the agents performing it do not identify themselves, unlike police prevention activities on the

[144] Art. 17 ICCPR, general comment No. 16 of the United Nations Human Rights Committee.

streets. Virtually any activity on the internet could be monitored by authorities for security purposes, and the individuals under surveillance would never be notified, making the activity resemble that of intelligence services far more than that of domestic security agencies.

Another potential infringement of human rights may occur when, in criminal proceedings, OSINT is used to obtain more information about a person than what is relevant and strictly necessary for the investigation. Online information should not be used to construct a "profile" of the accused. Otherwise, there is a risk that, by introducing elements unrelated to the facts under investigation, the impartiality of the judge may be compromised, thereby violating due process.

Finally, criminal intelligence conducted without a court order or a specific criminal hypothesis is less like "patrolling" the streets and more like a "fishing expedition," which is inadmissible under the National Constitution and international human rights treaties.

V.2. Impact on Freedom of Expression

The implications of OSINT practices on the right to privacy are intrinsically linked to the potential impacts they may have on freedom of expression. The Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights has stated that "Respect for online freedom of expression assumes that there is privacy for people's communications. Indeed, without a private sphere, free from the arbitrary interference of the State or private individuals, the right to freedom of thought and expression cannot be exercised fully."[145]

Article 13 of the American Convention on Human Rights and Article 19 of the International Covenant on Civil and Political Rights establish the right of every person to freedom of expression, which includes "the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice."[146]

---

[145] IACHR, (n. 91), p. 130, and IACHR, "Estándares para una internet libre, abierta e incluyente," report from the Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, OEA/Ser.L/V/II, CIDH/RELE/INF.17/17, March 15, 2017, para. 183, retrieved from: http://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf, last access: August 14, 2023.

[146] Art. 13.1 and 19 PICP.

Its provisions are fully applicable to the communications, ideas, and information that are disseminated and accessed through the internet.[147]

The internet in general, and social media in particular, cannot be viewed merely as "sources of information" (as is the case with other open sources such as books, academic publications, journals, etc., which are designed for that purpose). On the contrary, they are valuable civic spaces for democratic deliberation and exercising other rights, such as freedom of education and association,[148] which must be protected rather than suppressed.

There are studies that demonstrate the chilling effect that OSINT practices have on speech. People tend to remain silent if they know they are being watched, especially when posting content on social media,[149] particularly if they believe their speech could be subject to criminal prosecution.

In the specific case of online interactions, we believe self-censorship might occur in one of the following ways: i) Refraining from participating in discussions or expressing ideas; ii) Participating in discussions and expressing ideas but with caution, avoiding candidly sharing thoughts out of fear of reprisals for unpopular opinions; iii) Shifting from "public" discussions to private settings, such as engaging in private exchanges instead of open-access discussion forums or comments on public posts; or iv) Participating in discussions with restricted access, for example, by setting social media profiles to "private," allowing only certain people to view their contributions.

The long-term effects of this situation are even more concerning. Given the internet's central role in public discourse, such chilling effects would stifle democratic deliberation and civic participation. The right to access information on matters of

---

[147] IACHR, (n. 91), § 2. UN, Human Rights Council, "Promoción, protección y disfrute de los derechos humanos en internet," A/HRC/20/L.13, June 29, 2012, § 1, retrieved from: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_20_L13.pdf, last access: August 14, 2023.

[148] UN, General Assembly, "Promoción y protección del derecho a la libertad de opinión y de expresión," A/66/290, August 10, 2011, § 61, retrieved from: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/449/81/PDF/N1144981.pdf, last access: August 14, 2023, cited in IACHR, (n. 91), § 2.

[149] See, for example, Stoycheff, Elizabeth, "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring," in: Journalism & Mass Communication Quarterly, vol. 93, No. 2, 2016, pp. 296-311.

public interest would be undermined, significantly affecting the broad and robust debate required in a democratic society.

In this regard, in their "Joint Declaration on Surveillance Programs and Their Impact on Freedom of Expression,[150] the United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights stated that it is "concerning that legislation on intelligence and security has remained inadequate as new technologies have been developed in the digital era. It is especially concerning that indiscriminate access to information on communication between persons can have a chilling effect on the free expression of thought and the search for and distribution of information in the region." For this reason, they urged states to review relevant legislation and amend their practices to ensure compliance with international human rights principles. In turn, the effect of OSINT on freedom of expression directly impacts the exercise of political rights such as freedom of association, political and trade union affiliation, and the right to protest, and particularly undermines the ability of human rights defenders, political dissidents, civil society organizations, and others to organize and resist.

What has been stated so far should not be interpreted in a way that weakens the right of access to information or the collective dimension of the right to freedom of expression. In this regard, it is necessary to establish a differentiated regime for OSINT activities carried out by the state (or by third parties on its behalf). Specifically, it is essential not to interfere with the work of journalists, researchers, and academic institutions.

---

[150] IACHR, OAS, "Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión, Report by the United Nations (UN) Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights of the OAS, 2013, retrieved from: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&lID=2, last access: August 14, 2023.

VI. Conclusions

In recent years, there has been a growing trend in the region for authorities to attempt to monitor individuals' online activity in various ways for surveillance purposes. One such method, which gained particular notoriety, has been intelligence gathering based on open sources (OSINT).

Although presented under the label of "cyber-patrolling," it is an intelligence activity. While framed as a public security measure, this practice inherently requires collecting, processing, and analyzing vast amounts of information. Moreover, unlike street patrolling, it is carried out in secrecy by unidentified or undercover agents. Finally, unlike the patrolling of physical spaces, this digital surveillance has targeted specific individuals—that is to say, intelligence targets.

A second observation regarding OSINT in the region is that it is being carried out outside the bounds of the law or based on non-statutory provisions. In none of the countries studied does there exist a legal framework that establishes limits for this activity—prescribing when it is legitimate to carry it out, to what extent, and under whose authority. Where enabling regulations do exist, they fail to meet legal standards and have not been the result of prior legislative debate. Moreover, OSINT tools have been used to profile journalists, protesters, human rights defenders, activists, politicians, social leaders, academics, and online influencers.

Some governments in the region have acquired OSINT software for surveillance. Thus, under the pretext of "patrolling" the internet, states have expanded their technological capacities for control and surveillance. The resources and institutional capacities to oversee these activities have not scaled proportionally.

A further challenge in overseeing OSINT activities is the lack of transparency in how states conduct them. Such secrecy takes various forms. First, the very existence of the activity, and even the existence of enabling regulations, may be entirely concealed. In other cases, contracts for the acquisition of OSINT services or the software used to implement them may be classified or kept confidential, usually on grounds of national security. Finally, it is difficult for individuals to defend themselves against specific OSINT operations targeting them when such actions are not disclosed by the

authorities. In this way, the activity is conducted behind the backs of society, beyond public scrutiny, and even without the knowledge of those directly affected.

In some states, OSINT activity for surveillance purposes has been carried out systematically, while in others, it has occurred sporadically. In yet others, it is difficult to make a definitive assessment due to a lack of transparency. In any of these scenarios, conducting such activities in the absence of laws that align their practice with international standards has the potential to impact the human rights of the population. The unchecked expansion of state oversight over people's internet activity undermines the role of the web as a civic space for public deliberation and its effectiveness as a tool for activist groups and vulnerable communities. We must therefore foster inclusive stakeholder dialogue to guide legislative reforms that align these practices with constitutional and international human rights standards.

As a safeguard against rights infringements in OSINT operations, state conduct must satisfy the three-part test of legality, necessity, and proportionality, as established in International Human Rights Law. OSINT activity—even when carried out by the state—can have legitimate uses, such as journalistic work or criminal investigations. However, the lack of clarity regarding the functions being exercised when the state conducts OSINT (whether for investigation, preventive surveillance, or intelligence) increases the likelihood of rights violations. This requires clear legal boundaries for state powers and robust oversight frameworks governing the use of OSINT and related technologies.

The regulation of this activity must legally mandate specific protocols for collecting, processing, and deleting open-source information. Such regulation should define what types of data can be collected from open sources and the purposes of such collection. Additionally, it should ensure the protection of user privacy and allow all expressions permitted under local and international legal frameworks on freedom of expression.

The protocols must establish accountability principles, such as the publication of periodic reports detailing the practices carried out using digital open sources. Likewise, the protocol must comply with the principles outlined in personal data protection laws, where applicable, to ensure that data subjects can exercise their rights of access, rectification, cancellation, and objection.

Oversight mechanisms are essential to prevent rights violations in the use of OSINT techniques. These should include post-notification to citizens who have been subject to surveillance and disclosure of how their information was used, prior judicial oversight, and establishing clear sanctions for those who commit abuses.

Alongside the regulation of OSINT practices to prevent human rights violations, it is also essential to establish transparency and disclosure obligations in the procurement of technology or third-party services involving such practices. In this regard, it is essential to have access to existing contracts between states and private companies providing OSINT services, which should be widely disseminated and readily available, along with information about the allocation of resources and the expenditures incurred for these purposes. Furthermore, it is necessary to publish statistics on the specific instances in which OSINT has been conducted on individuals and, where possible, the reasons that justified such actions. Another area in need of improvement in government transparency is the frequent use of national security as a barrier to accessing information.

Finally, states that procure OSINT systems or services should be required to conduct privacy impact assessments, and the results of these assessments should also be widely disseminated.