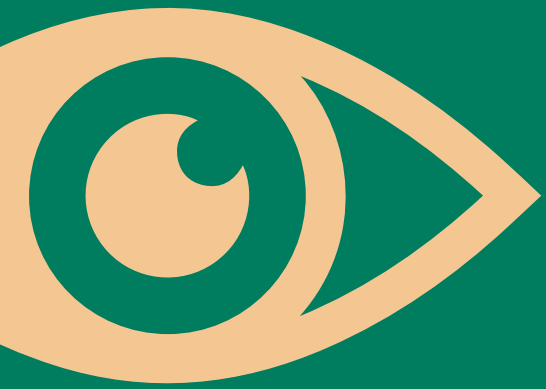
Public Politics on Law series / Editorial Dejusticia

STATE INTELLIGENCE GATHERING ON THE INTERNET AND SOCIAL MEDIA: THE CASE OF COLOMBIA



Lucía Camacho-Gutiérrez
Daniel Ospina-Celis
Juan Carlos Upegui-Mejía

Dejusticia

PRIVACY INTERNATIONAL

STATE INTELLIGENCE GATHERING ON THE INTERNET AND SOCIAL MEDIA: THE CASE OF COLOMBIA

LUCÍA CAMACHO-GUTIÉRREZ
DANIEL OSPINA-CELIS
JUAN CARLOS UPEGUI-MEJÍA

PRIVACY INTERNATIONAL

Editorial Dejusticia

In this report, we explore this subject by drawing on the "Secret Dossiers" case published in 2020 by *Semana* magazine, which shows how the Colombian state exploits social media and the internet in order to monitor and profile individuals.

Our analysis warns that the safeguards present in existing legislation are rather sparse and that intelligence agencies' desire to self-regulate on the issue of open source intelligence is almost nonexistent despite these agencies' surprising clarity about the data on the internet and the social media that interest them.

We believe that, in the discussion on desirable limits, the insights that have emerged regarding the passive monitoring of the electromagnetic spectrum and the interception of communications offer valuable lessons for better addressing the impact of online intelligence.

Keywords: Intelligence, internet, social media, privacy.

En esta investigación ofrecemos una primera aproximación a dicha materia a través del caso de las "Las carpetas secretas" publicado en 2020 por la revista *Semana*, que da cuenta de cómo la inteligencia colombiana explota las publicaciones en redes sociales, así como la información pública disponible en internet, con la intención de monitorear y perfilar a las personas.

La aproximación que ofrece este texto advierte que los límites de la legislación son más bien exiguos, y que la autorregulación de las agencias de inteligencia es casi inexistente pese a demostrar, al tiempo, una mayor claridad sobre los datos en internet y redes sociales que les resultan de interés.

Creemos que, en la discusión sobre los límites deseables, las reflexiones que han surgido respecto al monitoreo pasivo del espectro electromagnético y la interceptación de las comunicaciones ofrecen lecciones valiosas con las cuales se podría abordar mejor el impacto de la inteligencia en línea.

Palabras clave: inteligencia, internet, redes sociales, privacidad.

To quote this book:
Camacho-Gutiérrez, L., Ospina-Celis, D., & Upegui-Mejía, J. C. (2023). *State Intelligence Gathering on the Internet and Social Media: The Case of Colombia*. Dejusticia.

STATE INTELLIGENCE GATHERING ON THE INTERNET AND SOCIAL MEDIA: THE CASE OF COLOMBIA

LUCÍA CAMACHO-GUTIÉRREZ
DANIEL OSPINA-CELIS
JUAN CARLOS UPEGUI-MEJÍA

Public Politics on Law series / Editorial Dejusticia

Camacho-Gutiérrez, Lucía.
State Intelligence Gathering on the Internet and Social Media: The Case of Colombia / Lucía Camacho-Gutiérrez, Daniel Ospina-Celis, Juan Carlos Upegui-Mejía – Bogotá: Editorial Dejusticia, 2023.
56 pages; 22 cm. – (Políticas públicas al derecho)
978-628-7517-58-5
1. Intelligence 2. Internet 3. Social media 4. Privacy.
I. Tit. II. Series

ISBN 978-628-7517-58-5 digital version

Layout
Diego Alberto Valencia

Cover
Diana Gonzalez Molina

Translation and Copy Editing
Morgan Stoffregen

First edition
Bogotá, D.C., Colombia, November 2023

This text can be downloaded for free at
https://www.dejusticia.org

Dejusticia
Calle 35 # 24-31, Bogotá, D.C., Colombia
Telephone: (+57) 601 608 3605
www.dejusticia.org

Contents

Introduction 9

1. Internet and Social Media Intelligence: The Secret Dossiers Case 13
2. Regulation of (Online) Intelligence 15
3. The Practices of Intelligence Agencies 21
4. A Proposal to Advance the Discussion on Desirable Limits 36
5. Recommendations 46

References 49

The Authors

Lucía Camacho-Gutiérrez,

at the time of writing, was a Media Democracy Fund fellow at Dejusticia. She holds a law degree and a master's degree in human rights. https://orcid.org/0000-0002-9831-0255

Daniel Ospina-Celis

is a researcher at Dejusticia. He holds a law degree and a master's degree in history. https://orcid.org/0000-0002-0688-9854

Juan Carlos Upegui-Mejía

is a professor at the Universidad Externado de Colombia. Previously, he was a researcher at Dejusticia. https://orcid.org/0000-0002-4649-8217

Introduction

VOLVER AL CONTENIDO

The Colombian state conducts intelligence activities on the internet and social media. In general, these activities go unnoticed, and little is known about them. Occasionally, however, some cases come to light. In 2020, the journalistic investigation titled "The Secret Dossiers" ("Las carpetas secretas"), published by *Semana* magazine, revealed how some intelligence agencies were using the internet and social media to gather information with the objective of profiling journalists, political opponents of the administration, and human rights defenders.

State intelligence activities, when deployed legitimately, serve two basic purposes: to inform national security policy and to support military and police intelligence operations aimed at ensuring state and citizen security (Bruneau and Boraz 2007). Considering that intelligence work is essential for states, factors such as promptly obtaining actionable and reliable information allow the fulfillment of intelligence objectives and facilitate decision making.

In Colombia, intelligence activities have been regulated by law since 2013, when Law 1621 was passed. Under this law, the objective of the state agencies responsible for intelligence and counterintelligence is to protect human rights and prevent threats against the democratic order (Ley 1621 de 2013, art. 2).

To fulfill this function, intelligence agencies gather information from a variety of sources, including the internet and social media. The deployment of online information-gathering activities is not recent; according to data obtained in the course of this research, intelligence agencies have been regularly con-

sulting open sources such as the internet and social media since at least 2014 (the National Police) and 2016 (the National Army).

While individuals who use the internet and social media generally use them to communicate, study, engage in leisure activities, and search for information, intelligence agencies also use them to gather information that supports investigative hypotheses with an eye toward identifying, containing, and preventing possible security risks. In this sense, the internet and social media serve as sources of easily accessible information, particularly personal information, that is of interest for intelligence purposes.

The volume of information that can be accessed from open sources on the internet grows exponentially each day. Moreover, the personal information circulating on social media allows for detailed insights into the social circles, activities, tastes, and places most visited by individuals who are declared as intelligence targets. Currently, the internet and social media constitute two of the most attractive and cost-efficient methods for states to access strategic information (Akghar 2016; Marzell 2016; Steele 2007; Hassan 2019).

Internet intelligence is a subtype of open-source intelligence that involves the consultation, access, and use of information—free or for a fee—that is available online and unrestricted by privacy or copyright laws. That information is gathered, processed, analyzed, and interpreted in order to direct state action as it concerns national security and public safety (Akghar 2016; Gibson 2016; Miller 2018).

Social media intelligence is a type of online intelligence that occurs on platforms that facilitate the two-way and public interactions among individuals who publish personal information about themselves, what they think, with whom they interact, and what they do, in real time. Using and accessing social media to gather intelligence is valuable in that it contributes to identifying individuals and groups of interest to the state, preventing crime, and monitoring situations as they unfold (Omand et al. 2012; Omand 2017).

However, the ethical and legal issues that surround the

Colombian government's practice of accessing and using personal information that is available online have been widely understudied. The purpose of this report is to shed light on some of these issues, particularly those concerning the view of certain Colombian intelligence agencies that the information that is accessible on the internet and social media—by the mere fact of being available on these channels—can be used without limits or restrictions in the context of intelligence activities.

We are aware that using information that is available on the internet or social media can be highly valuable for citizens and even for the state in certain situations and under clear conditions. For example, investigative journalism that seeks to nurture public debate or provide evidence of human rights violations is a case of such information being used for legitimate and beneficial ends; another example is the use of such information by states to prevent terrorist attacks, dismantle human trafficking networks, or prevent child exploitation and abuse.

Naturally, there is a difference between investigative undertakings for academic or journalistic purposes and those conducted as part of state intelligence gathering. While any investigative effort that seeks to study, scrutinize, or curtail the abuse of power should respect the rights of third parties, intelligence activities should, additionally, conform to the principles of legality, necessity, and proportionality. Public servants and the state may act only within the limits set by the law and within the framework of their legal powers and functions. The purpose of these principles is to establish necessary limits to state action in order to prevent the deployment of activities with the potential to affect fundamental rights from turning into a source of abuse.

A discussion of the limits that are and should be placed on intelligence activities—activities that are now ubiquitous on the internet and social media—should begin by dismantling the narrative that the mere ability to find and access personal information online allows intelligence bodies to do virtually anything with that information. Information that is available online does not stop being private or sensitive personal information by virtue of its publication. As a result, the seeking out, processing,

VOLVER AL CONTENIDO

and storing of such information must be subject to, among other things, the rules that protect privacy and the principles set out in the legislation governing the processing of personal data.

To conduct this research, which seeks to explore the limits that are and should be placed on intelligence activities, we consulted a variety of official sources (such as laws, decrees, resolutions, and Constitutional Court judgments) and unofficial sources (such as media clippings and literature on intelligence on the internet and social media). In addition, we conducted interviews with experts who have advised intelligence agencies and with experts in investigative journalism, whose identities we have promised to keep confidential. We would like to thank these individuals for their generosity when meeting with our team. We would also like to emphasize the extreme difficulty involved in securing these interviews. Although we approached a dozen experts, only 20% of them agreed to speak with our research team.

As part of our survey of official sources, we submitted a dozen formal requests for access to information to several intelligence agencies in order to inquire about the impact of the use of the internet and social media in the exercise of these agencies' functions. In this regard, it is noteworthy that some of the entities that we contacted applied Law 1712 of 2014 (regarding access to public information) and provided us with valuable information for the preparation of this report. Although this is a step forward in terms of transparency on issues that, in the past, would have received dismissive answers without further explanation, we believe there is still a long way to go.

Full access to information on basic aspects of open-source intelligence gathering remains a challenge. This is illustrated, for example, by the divergent interpretations of "confidentiality" expressed by different members of the intelligence community with regard to sharing such information, which raises doubts about whether Law 1712 is being correctly interpreted and applied.

Although this disparate application of the law worked to our advantage, we believe that if one entity can release informa-

tion on an issue that others claim is confidential, perhaps such confidentiality can be challenged altogether—particularly in keeping with the principle that, in case of doubt, transparency should prevail over confidentiality.

This report is organized into four sections. In the first section, we revisit the Secret Dossiers case to illustrate the narrative behind the Colombian state's intelligence activities on the internet and social media. In the second section, we briefly describe the regulation of intelligence activities in Colombia, with an emphasis on the regulatory framework applicable to online intelligence. In the third section, we share our findings on the limits that some intelligence agencies claim to apply, the ambiguity that currently permeates this field, and these agencies' positioning on the nature of the information they obtain through intelligence gathering on the internet and social media. Finally, we outline a series of recommendations based on a careful consideration of the values at stake: the guarantee of national security and the enforcement of the constitutional and democratic order, on the one hand, and respect for fundamental rights, including privacy and data protection, on the other.

VOLVER AL CONTENIDO

1. Internet and Social Media Intelligence: The Secret Dossiers Case

In 2020, an investigation titled "The Secret Dossiers" was published by *Semana* magazine. This investigative report describes how the National Army had collected personal information on more than 130 individuals, including journalists, human rights defenders, union members and congressmembers, with the aim of creating detailed profiles of each person.

The Army collected this information through various means, including the internet and social media. According to *Semana*, the creation of these profiles and the analysis of the information did not serve a legitimate purpose, especially because designating individuals as targets of intelligence activities on the basis of their political affiliation, human rights work, or reporting is discriminatory, to say the least.

But this investigation goes beyond exposing the state's questionable criteria for selecting intelligence targets. As *Semana* showed, one of the journalists for whom an intelligence profile was created is a *New York Times* correspondent. The Army extracted information from his Twitter posts, identifying his followers, their home countries, and individuals in his immediate social circle and with whom he had frequently interacted. In fact, intelligence researchers also dug into the social media posts of some of his followers.

Another victim of illegal profiling was a photojournalist, on whom the Army obtained large amounts of personal information. It collected information based on her Facebook activity and closest contacts and drew up a profile for each of these contacts on the basis of their posts. The Army also collected geolocation information associated with each of the photos she posted on Instagram.

The *Semana* report also highlights the case of a Colombian journalist whose personal ID number (*cédula de ciudadanía*) was acquired, making it possible to search public databases accessible online. These databases allowed the Army to obtain information on her designated polling place, vehicle ownership records, and traffic offenses, which in turn revealed her home address, vehicles registered to her name, and routes traveled.

The report describes the arguments put forth by some of the country's intelligence agencies and experts:

> Some of those directly responsible, including colonels and generals, have tried to justify the profiles by arguing that the information was collected from open sources and social media.
>
> ***
>
> "[The military] is going to try to beat around the bush by arguing that information gathered from open sources is not intelligence per se. The problem with that is that the final product—in other words, the reports that are made based on that data—is in fact intelligence and has a specific purpose, which in this case is not clear …" explained a senior official of the National Intelligence Directorate to *Semana*. (*Semana* 2020a)

El País, another media outlet that sought the opinion of security experts on the Army's collection of information available on the internet and social media with the intent of profiling a particular group of individuals, reported that "all this data is on open sources on social media, so 'this is not espionage, it is not wiretapping. Surveillance is when you go after the person'" (*El País* 2020).

The common thread in these cases reveals a problematic baseline position: processing information available on the internet and social media, due to its publication and availability, is not subject to legal limits; the state considers such information to be public and freely accessible and searchable.

Since the information available on the internet circulates freely, it could be argued that an intelligence agency's access to and use of this information would not qualify as an intelligence activity per se. If anyone can access this information and use it for different purposes, its access is public. How can it be problematic, then, if intelligence agencies access information on the internet and social media? Why should we consider such activity as being subject to legal limits, even when conducted by intelligence agencies?

2. Regulation of (Online) Intelligence

The questions raised by the cases in the Secret Dossiers investigation—that is, questions concerning the apparently free or discretionary nature of any activity related to the collection and processing of information available in open sources, especially the internet—lead us to ask about the regulation of intelligence activities given that these activities are being conducted with increasing intensity in digital settings, namely the internet and social media.

What regulations exist in Colombia with regard to intelligence agencies' processing of information, especially personal information, that is available on the internet and social media? What (if any) limits apply to this activity? Is it true that intelligence agencies have total discretion to gather, process, and use personal information available on the internet?

VOLVER AL CONTENIDO

Colombian law does not provide definitive answers. Current regulations are sparse and do not appear to consider the potential, complexity, or risks of gathering and processing information from open sources on the internet and social media. This regulatory vacuum is compounded by a delegation of the regulation of intelligence gathering to the intelligence agencies themselves, without clear and uniform criteria. Let's take a look.

2.1 Intelligence Regulation and "Means" of Intelligence

Law 1621 of 2013, known as the Intelligence Law, was meant to bring order to an activity with a long history of abuse in Colombia; until 2013, intelligence and counterintelligence activities had been conducted by all presidential administrations without a clear legal framework and with high levels of discretion. Law 1621 sought to remedy this shortcoming by establishing a normative basis for the intelligence work carried out by different specialized agencies.

In Colombia, intelligence activities are performed by a variety of agencies in a compartmentalized manner, under a basic legal framework. These agencies include the following:

- → The Military Forces (National Army, National Navy, and Air Force)
- → The National Police
- → The National Intelligence Directorate (DNI)
- → The Information and Financial Analysis Unit

These entities make up the "intelligence community" and are empowered to conduct intelligence operations on the internet and social media. In 2011, for example, the DNI was granted authority to collect information through "technical means [and] open means" of information. And in 2013, Statutory Law 1621 granted the same authority to the rest of the intelligence community (Decreto 4179 de 2011; Ley 1621 de 2013). The legislation on the topic considers the internet and social media to be "means of intelligence."

However, the provision authorizing the use of these "means" does not include any definition of their scope. As a result of several access-to-information requests that we submitted to intelligence agencies for this report, we know that both the National Police and the DNI include the internet and social media in the "open media" and "technical media" categories.[1]

However, the Intelligence Law provides that the use of technical and open means is limited by the principles of suitability and proportionality, as well as the National Intelligence Plan.

The suitability principle requires that the means of intelligence that are employed must meet the intelligence goals set forth in Law 1621 of 2013 (ensuring the fulfillment of state objectives, guaranteeing national security, and enforcing the constitutional order and the protection of fundamental rights). Meanwhile, the proportionality principle seeks to ensure that the benefits obtained from the means of intelligence are greater than the restrictions placed on other "constitutional principles and values." And, of course, it calls for adherence to the Constitution and the law generally.

The National Intelligence Plan is an internal operational limit on intelligence activities that use "technical and open means." Its content is confidential, but it establishes, according to the national government, risks, threats, and intelligence priorities; the limits and goals that these activities should satisfy; and the parties responsible for its implementation (Ley 1621; Decreto 1070).

Thus, intelligence operations seeking to dismantle criminal gangs, for example, should have been outlined as intelligence requirements in the National Intelligence Plan in order to be carried out.

The order to conduct an intelligence operation should be consistent with the priorities and needs established by the national government. This acts as a limit on the initiation of intelligence operations that may appear suitable and proportional but have not been planned.

---

1 See replies to file nos. DIPOL-ASJD-13 (June 10, 2022) and 2-2022-139C (June 14, 2022).

Despite its importance, the National Intelligence Plan is not meant to anticipate the means of intelligence that will be employed, since the selection and deployment of such means is the responsibility of those who set specific intelligence requirements, authorize intelligence operations, and execute these operations.

2.2 The Next Step: Intelligence Manuals and Protocols

Law 1621 of 2013 is very broad when it comes to defining the specific limits to intelligence activities that use technical and open means; it is merely a starting point. The specifics of these limits are left to the intelligence agencies. This function falls within intelligence agencies' authority to issue their own manuals and protocols, which includes the possibility of specifying the limits that apply to the use of means such as the internet and social media.

From the outset, this institutional design has meant that regulations on gathering and processing information available on the internet and social media can be as numerous and diverse as the agencies that make up the intelligence community.

The Intelligence Law and Decree 857 of 2014 provide that manuals and protocols should observe the Constitution and the law generally, but the confidential nature of their content prevents understanding how such observance takes shape at the legal level or in the adoption of methodological or technological limits.

Moreover, not even the intelligence manuals that are available on the internet are specific enough about the limits placed on their activities, particularly when it comes to "technical and open means" such as the internet and social media. The intelligence manuals of the National Police and the National Army are an example of this situation.

Both of these manuals allow the possibility of using the internet to carry out intelligence activities. However, they do not specify the legal limits of such activities by considering the technical and legal aspects of the internet and social media. We

ask ourselves, then, what protection or safeguards are afforded, for example, to online interactions that take place in private groups on a social network or that are protected by privacy settings? What personal information is excluded, or should be excluded, from being sought or accessed in the course of intelligence gathering? The manuals do not address these types of questions. They merely state that the Constitution and the law must be respected.

The National Army's *Fundamental Intelligence Manual*, which dates back to 2016 and is available on the internet through channels other than the entity's official website, does not have specific provisions on the collection and processing of information gathered from the internet and social media for intelligence purposes. The manual and its revised edition simply provide for the use of open-source intelligence along with other sources that, as a whole, are necessary "to assist in understanding the situation, supporting the development of plans and orders and responding to information requirements" (Resolución 01886 de 2016; Resolución 01869 de 2017).

In fact, the National Army's manual does not mention any limits associated with the deployment of intelligence activities on the internet or social media, despite being directed at intelligence officers in training. A not insignificant fact concerns the absence of reference to social media as a means and source of intelligence information, especially since evidence exists that these platforms have already been used by the National Army, as revealed by the Secret Dossiers case. This situation leads us to wonder whether other sources of information not included in the manual are used, whether the army establishes any difference between social media and the rest of the internet, and whether the differences between one and the other should be subject to special consideration for intelligence purposes.

In addition to these regulatory particularities, lawmakers, when issuing the Personal Data Protection Law, decided to exclude intelligence and counterintelligence activities from the law's scope (Ley 1581, art. 2). However, this exclusion does not mean that there should be no special regulation of these activi-

ties. The Intelligence Law, issued a year later, in 2013, is silent on the matter.

Although databases with intelligence and counterintelligence information are excluded from the application of the Personal Data Protection Law, general data processing principles apply to them (Ley 1581, art. 2).

Naturally, only some of these principles apply since intelligence is not an activity consented to by the individual, and therefore a person could not oppose the collection of their personal information—thus, the principle of freedom is left out of the discussion. However, to date, neither legislation nor constitutional jurisprudence has specified how the other principles—such as the principle of access and restricted circulation of information or the principle of transparency, accuracy, and quality of information—would be operationalized or to what extent an individual could exercise the right to control their information and the rights facilitated by habeas data.

***

State intelligence activities with the net effect of intruding on online privacy demand clear limits. These are activities that by definition seek to extract information from the original medium in which it was published and then use it without the knowledge of, and for purposes not intended by, the individual, possibly aggregating this information with other public (such as state-run databases) and private sources of information. Such information gathering enables the profiling of an individual and supports the elaboration or verification of hypotheses with great potential to affect or harm that person.

It is also insufficient to attempt to set these limits by allowing each intelligence agency to draft its own manuals and protocols, as is currently the case in Colombia. This is so for two reasons: because there are no commonly shared, more precise rules to which the procedures regulated this way should adhere to, and because the idea of self-regulation is at odds with the inherent biases of intelligence gathering and with the natural desire of the Colombian state to conduct these activities without legal limits or external controls.

Finally, defining these limits poses the challenge of specifying what is, or what should be, the scope of the expectation of privacy on social media and, in general, on the internet—especially considering that intelligence is an activity that does not require the consent of the individual for its deployment. By definition, intelligence is carried out without the individual's knowledge, and its nature, methods, and procedures prevent individuals from exercising any recourse aimed at controlling the information collected about them.

VOLVER AL CONTENIDO

3. The Practices of Intelligence Agencies

For more than five years, the Colombian state has been systematically collecting information from the internet for intelligence purposes. The intelligence agencies and experts consulted for this report acknowledge that this is a common practice. Although the basic regulatory framework on intelligence activities dates back to the formal emergence of these practices, this framework is neither sufficiently specific nor exhaustive with regard to the particularities of carrying out intelligence activities on the internet and social media.

In an attempt to compensate for this absence of normative criteria at a general level, Colombian law confers to intelligence authorities the power to issue their own operational manuals. This enables a sort of self-regulation at the technical and operational levels regarding the means and practices used to accomplish these authorities' legal and constitutional functions of protecting national security.

Naming and recognizing these practices—as we observed in the replies to the requests for information that we submitted—seems to function as a proxy for regulation. Even so, the conclusion does not change: the limits remain vague, which results in a high level of arbitrariness regarding how these activities are conducted.

In this section, we explore the reasons and purposes of intelligence gathering on the internet and social media and the limits that some Colombian intelligence agencies claim to apply

to their work. We also present information on how they train their personnel regarding the application of these limits and what intelligence information they seek to obtain from the internet and social media.

As we will see, the limits are vague, and the training processes seem to reiterate abstract formulas on adherence to the law, which does little to guide the activity or prevent unwarranted intrusions into people's private lives. For example, they do not clarify whether it is possible to extract intelligence information from groups or private accounts on social media or whether personal information contained in public databases run by the state can be used for intelligence purposes, a purpose clearly not foreseen or informed to the public at the time of these databases' creation.

We will also see that, compared to the vagueness of the limits, there appears to be greater certainty about what online information is of interest to the state. However, there is no evidence of special classification practices or of the differential treatment of public, private, or sensitive personal information collected on the internet and social media. The latter is revealing about the status of the discussions on privacy and the processing of personal data by intelligence agencies.

3.1 The Objectives of Intelligence Gathering on the Internet and Social Media

According to our interviewees, intelligence gathering on the internet and social media illustrates the context for conducting this type of activity. The context is part of the first phase of the intelligence cycle: planning. This helps organize efforts in the following phases of intelligence gathering, which are aimed at collecting, storing, processing, and analyzing the information obtained. As noted by one of the interviewees, "Without context, this task cannot be enriched."

The context information drawn from the internet and social media seeks to answer basic but decisive questions in relation to an individual: who the person is, whom they interact with, the strength of these connections, what the person's past

activities have been, their occupation, their background, the circles in which they exert influence, their personal knowledge, etc. This, in turn, helps advance more concrete hypotheses: the relationship that may exist between this individual and critical events in terms of citizen security, national security, or national defense. Before the internet, this information was acquired from traditional open and public sources—the written press, radio, television, academic journals, books, and gray literature—or through secret or covert sources, which are much more costly and risky compared to gathering information that is available online.

As noted by one of the experts interviewed for this report, thanks to the massification of the internet and the digitalization of the vast majority of traditional public and open sources, "it could be said that 80% of the intelligence [in Colombia] today is obtained online." Numerous authors embrace a similar diagnosis regarding other countries (Steele 2007; Pallaris 2008; Marzell 2016). But the information that is available online is not just a key source of intelligence—even the *absence* of such information about a person of interest could become a reason for suspicion because "whether we want to or not, we all have a digital footprint on the internet," noted the same interviewee.

While interviewees are not certain about how this activity is conducted by intelligence agencies in Colombia—that is, whether it is done manually or through the use of certain technologies (APIs on social media, web scraping, etc.)—they agree that its use today goes far beyond the interests and actors relevant to the protection of national security and defense. In other words, the internet and social media are being used for criminal investigation and "cyber-patrolling," as well as in the context of government communications strategies.

Indeed, two of our interviewees stated that government officials seek to collect information available online, especially on social media, to map the issues and actors involved in public debates. These efforts are framed within communications strategies whose objectives are, among other things, to measure the possible success of certain public policy decisions or even to

improve the president's public approval rating.[2] In other words, such information gathering is carried out by certain administrations, but not in the context of a "state" activity.

In this regard, the contract signed between the Administrative Department of the Presidency and the Du Brands company is particularly illuminating. This contract sought the "creation of communications strategies for media outreach, content production and administration of Duque's and the presidency's digital channels." The strategies deployed by Du Brands included "the parameterization of social media users [and] media monitoring" (Fundación para la Libertad de Prensa 2020, 38).

The activities deployed on social media by Du Brands and those carried out by intelligence agencies share a common element: the monitoring of online activity in order to profile a group of individuals, including through the identification of their circle of followers on a given social media channel. In both cases, contacts and followers shed light on "who is who" based on their opinion of the administration (in the case of Du Brands) or based on the security risk they represent (in the case of intelligence agencies).

In both cases, public and private data (and sensitive data, such as those reflecting one's political stance) are obtained from the internet and social media without the consent, knowledge, or authorization of the person who published content freely as part of the exercise of their right to freedom of expression and opinion. The expectation of privacy of an individual who decides to publish personal information is, in this case, to interact in a public forum, not to be subject to monitoring and profiling by the administration currently in power.

One of the tweeters who was described as "negative" by Du Brands—due to his criticism of the administration—filed a *tutela* to protect his rights to privacy and to habeas data. The case was

2 In its research on the United Kingdom, Privacy International (2020) reports on the state's use of social media intelligence to inform decision-making on children's social services, to monitor social protest, to recover unpaid taxes, to detect the advertising of illegal goods, and to confirm the veracity of information provided by social benefit claimants, among others.

decided by the Supreme Court of Justice, which held that sensitive information published on Twitter by an individual, in the exercise of the right to freedom of opinion on the internet, cannot be used in data processing activities that have not been freely and previously consented to by that person. The mere fact that sensitive data are published online and easy to access does not grant permission to third parties, such as the government, to use such information indiscriminately for purposes such as improving the president's public image (Supreme Court of Justice 2020).

In this regard, one of the experts we interviewed stressed the importance of distinguishing between *intelligence* activities and *investigative* activities on the internet and social media in order to regulate the processing of personal information. Personal information collected and processed during intelligence activities is subject to the intelligence cycle and is intended to be consumed by high-level intelligence officials in order to guide security-related decision-making. These activities are arguably very different from activities relating to investigative journalism or political or commercial marketing firms, such as those carried out by Du Brands in the aforementioned contract.

On the issue of intelligence gathering on the internet and social media, interviewees emphasized the need to discuss the limits that should apply to the state's intelligence activities. It is necessary to have clarity about which objectives are valid in this regard; the limits that should apply to the state's collection of public, private, and sensitive information that is available online; and the storing and processing of such information. Indeed, these issues emerge as priorities in the following sections.

3.2 Practices without Clear Boundaries

The Intelligence Directorate of the National Police (DIPOL) acknowledges that it does not distinguish between the physical and the digital environment when it comes to gathering information for intelligence purposes. DIPOL considers that intelligence activities on the internet and social media serve the same purpose as in the analogue world: to identify "phenomena and threats that may threaten the constitutional values

of the constitutional and legal framework, democratic rule, and national security and defense."[3] These activities "are carried out regularly," and their use depends on "the conditions that arise in each case,"[4] which prevents a determination of whether searching open sources outweighs using other sources of information. A similar situation exists at the DNI, which claims to conduct intelligence activities on the internet and social media in order to fulfill its legal and constitutional functions.[5]

Both the DNI and DIPOL repeat the mantra of upholding the Constitution and the law. As noted in its replies to our requests for information, DIPOL claims to comply with the principles of suitability, necessity, and proportionality; the priorities provided for in the National Intelligence Plan; and the limits provided for in its orders and work missions.[6] The DNI, meanwhile, claims to have no internal guidelines for open-source intelligence gathering.[7]

Both intelligence agencies[8] point to the role of the data protection centers that exist in all intelligence agencies and which are responsible for curating the intelligence information that is collected. These centers are charged with three duties: (i) ensuring that the processes of collecting, storing, and processing intelligence information are compatible with the law; (ii) ensuring the exclusion of information that was gathered but is not compatible with the law; and (iii) ensuring that the storage of intelligence information meets the criteria of neutrality and nondiscrimination.

While this mission is undoubtedly critical, the scope of these data protection centers is limited. They do not grant data subjects access to the information that identifies them as an

3 See file no. GS-2022/DIPOL-ASJUD-13 (June 10, 2022), p. 4.

4 See file no. GS-2022-028515/DIPOL-ASJUD-13 (September 5, 2022).

5 See file no. 2-2022-139C (June 14, 2022), p. 2.

6 See file no. DIPOL-ASJUD-13 (June 10, 2022), p. 3.

7 See file no. 2-2022-139C (June 14, 2022).

8 See file nos. 2-2022-2113 (August 29, 2022), p. 2; GS-2022-028515/DIPOL-ASJUD-13 (September 5, 2022), p. 2.

individual and was collected for intelligence purposes, nor do they allow data subjects to request the correction of personal, private, or sensitive information that is inaccurate, outdated, or erroneous—much less to request the removal or purging of intelligence files that contain information collected without regard for the principle of legality or that has already fulfilled its cycle and utility.

3.3 Training of Intelligence Agents

Another key issue is the training and qualification of intelligence personnel. Training is critical not only to the success of intelligence gathering but also to its correctness, which is obligatory according to Law 1621 of 2013. This law specifies two critical roles for training: (i) to instruct how intelligence tasks are carried out and (ii) to instruct on the boundaries that define the correctness and legality of such activities.

Understanding intelligence agents' training also makes it possible to understand how these agents are working to comply with constitutional and legal requirements, especially when, in their role as investigators, they perform an activity that is not subject to external control, review, or audit—at least not of a preventive nature.

The fact that DIPOL's School of Intelligence and Counterintelligence does not have seminars dedicated to intelligence gathering on the internet and social media "does not mean that the collection of information from open sources or social media is not a topic of study, as it is implied as a source of information [to be studied] in the gathering component."[9]

In its replies to our requests for information, DIPOL attached several reading materials from its training workshops. The first one was on "the function of intelligence and counterintelligence in the Colombian state" and the second was on "limits of the intelligence and counterintelligence function, purposes, principles and controls."[10]

9 See file no. GS-2022-001408/DIREC-GUSAP-29.25, p. 4.

10 See file no. 2-2022-2113 (August 29, 2022), pp. 12 et seq.

The second text is exhaustive in its review of constitutional jurisprudence and current regulations on the subject of intelligence. It mentions the importance of applying the principles of suitability and proportionality, but not how this task should be achieved in practice. The text emphasizes the need to protect individuals' privacy but does not specify what steps or precautions should be implemented to this end.[11]

In other words, these materials do not seem to represent genuine pedagogy on the applicable limits but rather the reiteration of valuable but vague formulas that are left largely unexplained, especially considering that the content of these training workshops—which is focused on the development of skills needed for the execution of a specific task—should be as precise as possible.

The DNI has a training cycle called "Open Sources" that is taught approximately four times a year, but its contents, teaching strategies, and assessment process are confidential.[12]

3.4 Partial Certainty about Information Extracted from the Internet

In the context of the overall uncertainty surrounding the limits that should be placed on the collection and processing of personal information for intelligence purposes, there is somewhat more certainty about the information that some of the intelligence agencies gather on the internet and social media. Yet it is only a partial certainty, because when asked if they make any distinction between public, private, or sensitive data collection and processing, our interviewees were not specific in their answers.

DIPOL, for example, asserts that it collects "open data"—an expression it uses as a synonym for content published online—which constitutes the first "input for the generation of knowledge" for intelligence. DIPOL claims to consult, in general, all digital environments that are publicly accessible on the

11 Ibid.

12 Ibid., p. 1.

internet, "without being limited to a pre-established listing or website for collection activity."[13]

The DNI, for its part, notes that it consults publicly available and open sources of information, which "include social media, blogs, magazines, [and] newspapers," for information on persons and entities of interest. It does not restrict its consultations to specific websites or platforms. It does claim, however, that these consultations are limited to "what is strictly necessary to accomplish the function" of intelligence.[14] Moreover, it notes that consulting open sources "is virtually unlimited," so it can "outperform queries in other sources of information."[15]

That said, the distinction between the types of personal data they expect to extract from the internet is not a trivial one, since it has an impact on the "delimitation and identification of both the persons and the authorities that are legitimized to access or disclose such information" (Corte Constitucional, Sentencia T-729 de 2002).

The Constitutional Court has stated that "any person, directly and without the obligation to satisfy any requirement," may access personal data that is public or held by the state. With regard to public personal data, the data subject cannot oppose the lawful access of third parties, even though that person has the right to request that their data be updated, rectified, or eliminated (as long as the person does not have a legal or contractual obligation to remain in a given database) (Corte Constitutional, Sentencia T-729 de 2002).

Private and sensitive personal data, on the other hand, entail more stringent legal barriers to access for third parties. Even when these data may be published on the internet, their nature does not change—that is, their publication does not transform them into public data (Superintendencia de Industria y Comercio 2022). And they can only be offered to third parties pursuant to "the order of an authority discharging their duties or within

13 See file no. DIPOL-ASJUD-13 (June 10, 2022), p. 2.

14 See file no. 2-2022-139C (June 14, 2022).

15 See file no. 2-2022-2113 (August 29, 2022), p. 1.

the framework of the principles of personal data management" under the responsibility of the data controller (Corte Constitutional, Sentencia T-729 de 2002).

Likewise, the aggregation of public, private, and sensitive personal data, even when it is facilitated by state-of-the-art technology, is prohibited[16] because such bundling contributes to the creation of "virtual profiles," which goes against the principle of the individuality of data. Hence, cross-checking databases requires express authorization (Superintendencia de Industria y Comercio 2020; Corte Constitucional, Sentencia C-748 de 2011).

When asked if in the course of its intelligence activities it makes any distinctions between the nature of the data it collects online, the DNI said that it accepts the contents of the Financial Data Protection Law and the Personal Data Protection Law. According to its response, "It is important to emphasize that [the] exception to the processing of personal data provided for in Laws 1266 of 2008 and 1581 of 2012 does not prevent intelligence agencies from indiscriminately using the personal data collected."[17] With respect to the possibility of recognizing the data subject's right to exercise control over their information, the DNI indicates that "the exercise of the personal data processing regime is not applicable to citizens when personal data have been collected by state security agencies for the purpose of internal and external national security and defense."[18]

For its part, DIPOL affirms that in terms of personal data, it accepts "the nature, character and condition that existing norms establish for the national territory" but that "the provisions

16 Although the Superintendence of Industry and Commerce and the Constitutional Court agree that aggregating data is a prohibited activity, we believe that the dynamics of data processing in the digital world make aggregation a necessary condition because the processes of prediction and inference of other data depend on this practice. Changing the meaning of this criterion would require, among other things, opening a discussion on updating the data protection regime, which, at least for now, does not appear to be on the horizon.

17 See file no. 2-2022-2113 (August 29, 2022), p. 3.

18 Ibid., p. 4.

of [the General Law on Data Protection] will not be applicable."[19] Does this mean that the directorate does not apply the Personal Data Protection Law but, at the same time, embraces the distinction between private and sensitive data set forth in that regulatory framework? DIPOL's position is confusing. In addition, in terms of the rights of the data subject, it confines itself to recognizing the role of data protection centers in the processing of data, whose limitations are highlighted above.

These entities' replies suggest the need to revisit debates that have apparently been concluded but which merit further examination. For example, if intelligence cross-checks seek to infer data to corroborate certain hypotheses, what is the legal basis to justify database cross-checks that may generate potentially negative legal effects for the data subject? Moreover, why should the nonconsensual nature of intelligence work necessarily translate into the data subject's inability to exercise any control over their personal information, even with respect to information that is public?

Furthermore, can intelligence agencies access and use at their discretion public data managed by the state at any time and for any reason? And what restrictions, if any, should apply to public personal data that are collected and processed for intelligence purposes simply because they are accessible online?

3.5 Cyber-Patrolling

Cyber-patrolling is a set of activities directed at identifying cybersecurity threats and incidents, as well as detecting breaches of the availability, integrity, and confidentiality of information that circulates on the internet (Resolución 5839 de 2015).

According to official information, cyber-patrolling[20] in-

19 See file no. GS-2022-028515/DIPOL-ASJUD-13 (September 5, 2022), pp. 2–3.

20 We would like to thank FLIP (Fundación para la Libertad de Prensa) for sharing the state's responses to the requests for information that it submitted in 2021 regarding the deployment of cyber-patrolling actions in the context of the social protests that took place in May of that same year.

cludes the consultation, observation, and collection of open and public data and content on the internet and social media "without any restrictions or privacy settings."[21] The data that are of interest are those that shed light on the impact of a particular social media post, such as "counts on the number of posts, interactions and visualizations offered by social media channels and web pages themselves."[22]

The collection of personal information on the internet, in the context of cyber-patrolling, is based on an assumption regarding what is public and open on the internet and social media. Although technical limits—such as the privacy settings that users apply to their accounts—can affect these activities, the regulation and scope of these activities are no more precise than those regulating the activities of intelligence agencies.

Cyber-patrolling is carried out by the Cybernetic Center of the National Police, which is attached to the criminal investigation unit of the National Police. For the purposes of this entity, cyber-patrolling is not considered a police intelligence activity but rather a criminal investigation activity. The crux of the matter is that this activity takes place online and involves monitoring the internet and social media, as well as accessing and processing personal information accessible through these mediums.

An exploration of cyber-patrolling allows us to understand the vision and capabilities of some authorities in relation to the act of consulting the internet and social media in order to gather information of interest. But, above all, it points to a key task for defining the activity: specifying the very notions of intelligence on the internet and social media and pointing to the aspects that warrant regulation.

The distinction between intelligence and criminal investigation activities has already been explored in the past by the Constitutional Court, which makes this distinction on the basis of two criteria. The functional criterion, according to which

21 See file no. GS-2021-108176-DIJIN-CECIP 1.10 (August 24, 2021), FLIP, p. 1.

22 See file no. GS-2021-DIJIN-CECIP-1.10 (June 30, 2021), FLIP, p. 5.

intelligence activities seek the protection of broad general interests—such as the enforcement of the constitutional order or national security—guides the prevention, control, and neutralization of threats and supports hypotheses of the operations that inform the state's decision-making process. And the second is the evidentiary value criterion, according to which intelligence information does not have evidentiary value in judicial matters (Sentencias C-913 de 2010 and C-540 de 2012).

Criminal investigations, on the other hand, focus on gathering evidence that can be assessed in a trial, before an independent judge, to ascertain the potential criminal liability of a person. In addition, because of its special evidentiary role, this information should be prepared in accordance with the rules of due process, and it is subject to contestation. Although it is true that intelligence information can be used in criminal investigations, it has the capacity to serve only as a "guiding criterion," not as evidence (Ley 1621 de 2013; Corte Constitutional, Sentencias C-913 de 2010 and C-540 de 2012).

***

Based on the replies we received from intelligence agencies and other public authorities, we can offer various preliminary conclusions that reveal a complex scenario that transcends the drafting of the Intelligence Law.

First, the state appears to operate under the assumption that all personal information accessible or available on the internet is synonymous with public personal data and may be used without limit or restriction. This premise serves to dismiss any relevant distinctions regarding personal data and their effect on the value associated with the protection of privacy. Such an understanding of personal information prevents individuals from exercising any kind of control over personal information that concerns them.

Second, the exception afforded to intelligence agencies to not apply the Data Protection Law generates interpretations that not only are confusing to the public but also do not converge, even among intelligence agencies themselves. This exception has been in force for a decade; however, there is no clarity

on how intelligence activities should apply the principles of data protection applicable to the regimes that are exempt from this law. Nor is it clear who is responsible for ensuring safeguards in the law's application.

Regarding this latter point, we asked the Office of the Attorney General whether, as part of its role as the data protection authority for public entities, it monitors the application of data protection principles by intelligence agencies. The office replied that it "does not have the authority to hear this matter."[23] This statement was made just as the internal resolution regulating the exercise of these powers was repealed by the Office of the Attorney General itself in May 2022. This is extremely concerning and is a clear sign of the precariousness of the mechanisms designed to exercise external, preventive, and independent control and monitoring over national intelligence activities.

Third, although intelligence agencies claimed privilege on different points that we inquired about, arguing that such disclosure would result in reasonably foreseeable harm, it is clear that raising subject-matter privilege is still a subjective endeavor. For example, the DNI invoked privilege in relation to the information pertaining the training of its personnel, information that was amply provided by DIPOL.

Fourth, and equally important, we wish to highlight the difficulties associated with understanding intelligence governance in Colombia. It is not easy to understand how intelligence agencies are organized internally or how they collaborate with one another, including how the intelligence community (which implements its own activities) relates to the Joint Intelligence Board (which determines interagency cooperation as it relates to intelligence).[24]

---

23 See Oficio 1135 (June 1, 2022).

24 The board's members include, among others, the minister of national defense, the high security advisor, or the official at or above the advisory level appointed by the president; the vice minister of national defense; the head of joint intelligence, representing the general commander of the Armed Forces; the head of army intelligence, representing the commander of the Armed Forces; the head of intelligence of the Navy, representing the commander of the Navy; the head of intelligence of the Colombian Air Force, re-

For example, we asked the Joint Intelligence Department of the General Command of the Military Forces[25] whether, as a result of the application of Law 1621 of 2013, it relies on intelligence obtained from the internet and social media, to which it replied that it did not, since this activity is not part of its functions.[26] To appreciate this answer, we must turn to the distinction between the *production* of intelligence information—which is the responsibility of the intelligence community only, and where decisions are made about the methods of collecting information—and the *consumption* and *sharing* of the analysis of intelligence information—in which the Joint Intelligence Board participates.

However, do the highest military commanders have the responsibility to know which sources of information are used by the intelligence community in its operational tasks? And does the principle of compartmentalization of information inhibit the Joint Intelligence Board from knowing which methods of intelligence are used during an operation? The confidentiality of (almost) everything related to intelligence activity prevents us from delving into these questions.

Finally, the experts interviewed agree that intelligence gathering on the internet and social media requires clear legal boundaries that go beyond the open-ended formulas that mandate the observance of the Constitution and the law. Additionally, they believe that the boundaries should seek to harmonize interests related to the protection of individuals' privacy with the exercise of the state's functions.

Tempering expectations on what is achievable through limits on the exploitation of the internet and social media is another point on which interviewees agree. They will be lowered until, for example, the practices and criteria for identifying inte-

---

presenting the commander of the Colombian Air Force; the director of police intelligence, representing the director general of the National Police; and the director of the Information and Financial Analysis Unit or their representative.

25 Which is also a member of the Joint Intelligence Board.

26 See file no. 0122006705402/MDN-COGFM-JEMCO-SEMOC-CGDJ2-OASPP-1.10 (June 9, 2022).

lligence targets do not have external and independent oversight and control mechanisms.

Declaring journalists, human rights defenders, or members of political parties as targets of interest is highly problematic and, prima facie, illegal, according to the provisions of the Intelligence Law. Additionally, profiling such individuals, based on their categorization as alleged threats to national security, is clearly illegal.

Of course, the discussion on means of intelligence leads to a recognition of the structural flaws of the Colombian intelligence community in relation to the mechanisms for internal, judicial, disciplinary, and political control (the latter of which is the responsibility of Congress and which, owing to issues related to its members' security clearance, has not been able to hold a single session), the deviation of intelligence resources, and the opaque acquisition of mass surveillance technologies, among others.

VOLVER AL CONTENIDO

4. A Proposal to Advance the Discussion on Desirable Limits

Against this backdrop—the relative novelty of intelligence activities that use open sources (specifically the internet and social media), the absence of regulation, what intelligence practices reveal in terms of how they understand the object (personal information available in open sources), and the laxity of existing limits—we must ask ourselves, What needs to be done to ensure the legitimate use of intelligence that is deployed on the internet and social media?

First, we should begin by recognizing that regulation of the right to the protection of privacy should apply to any activity that takes place in, or through, digital settings. We should also accept that intelligence gathering on the internet and social media is an activity that uses these mediums as more than a mere source or method of information. The internet and social media are spaces with specific architectures, policies, and actors that should be considered when deploying and regulating intelligence activity.

Second, we should consider the nature of open-source intelligence and take care not to mischaracterize it along the way. Information that is neither public nor open and that intelligence agencies seek to exploit is a type of intelligence whose effects also warrant analysis and whose particularities should be taken into account in order to regulate the activity as a whole.

Third, we should promote the recognition of the right to the protection of personal data vis-à-vis agencies that conduct intelligence activities through open sources and vis-à-vis the information thus gathered and recorded in intelligence files. It is essential to design clear rules that define the timing and scope of the legal mechanisms that allow individuals to know what information is collected from them by intelligence agencies, how it has been collected, to what end, and under what procedures.

In particular, this effort should be based on the duty to facilitate access and the effective delivery of personal information gathered from open sources or social media and which has been requested by the data subject. The reason is simple: information that was collected and processed under the assumption of being public, or information obtained in the media or from open sources, should not be privatized or made confidential after it has been collected, much less with respect to the data subject.

On this point, as noted by United Nations Special Rapporteur on human rights and counter-terrorism Martin Scheinin, good practices on the promotion of human rights by intelligence services recognize that although a claim of confidentiality of information may seek to protect the state's ongoing investigations, sources, and methods, this claim is not incompatible with the right to access personal information regarding investigations that have already concluded or that have completed their cycle and usefulness, even in relation to information held in intelligence archives.

Good practices reinforce the idea that access to personal information is "a safeguard against abuse, mismanagement and corruption … [that] assists in developing citizens' trust in Government actions" (Scheinin 2010, para. 40). These good practices can be adopted through legislation and have already been

reflected in constitutional jurisprudence—specifically judgment C-540 of 2012, which upheld the constitutionality of the Intelligence Law.

4.1 Online Privacy

In contrast to the position held by some intelligence experts and agencies, personal information published on the internet is not, by virtue of its being published, information that can be used by the state in any manner and for any purpose.

This position suggests that publishing on the internet implies completely relinquishing the possibility of controlling one's own information and asserting the protection of one's private life as a fundamental right. According to this position, personal information—whether sensitive, private, or public—can be freely accessed and processed by intelligence agencies, which shifts the burden of protecting this information to individuals. In addition to being controversial, this position aims to conceal a more important substantive discussion: the one on necessary limits on intelligence activity.

Indeed, the possibility of controlling one's own information, as an expression of the fundamental rights to identity, personal freedom, and the protection of privacy, exists both online and offline, as has been recognized by the Constitutional Court.[27] The fact that an individual's personal information is available online, for a variety of reasons and in different ways, does not imply that an individual loses the legal power to con-

27 In fact, the court held more than two decades ago that "the mandates expressed in the Constitution take on a substantial significance that demands from the constitutional judge the protection of the rights held by all persons, since these are guarantees that are also applicable in this area. There may be a virtual reality on the internet, but this does not mean that the rights, in this context, are also virtual. On the contrary, they are not virtual: they are express guarantees whose effective enjoyment in the so-called cyberspace must also be ensured by the constitutional judge" (Corte Constitucional, Sentencia C-1147 de 2001). This distinction between online and offline rights has also been eliminated by UNESCO's Charter of Human Rights and Principles for the Internet (Internet Rights & Principles Coalition 2015).

trol it or to intervene when it is being used in activities or circumstances that affect or could potentially affect the them.

For example, a person who decides to share on social media their position on the current administration, as well as information about the places they visit, does not have the option of controlling against possible unintended or unwanted uses of this information by third parties, especially the state. The privacy settings that can be adjusted on one's social media account are technical limits that can be easily overcome by intelligence investigators by sending a friend request or by following the account through a fake profile whose intentions are unknown by the person who owns the account.

Merely being available on the internet does not mean that information that could be considered private and sensitive (because of the potential for discrimination that gathering it entails for the data subject) loses its nature[28] or that the data subject loses the opportunity to demand restrictions on its use or the right to prevent it from being processed for unlawful or unconstitutional purposes.

By "processing," we refer, under Colombian law, to both gathering information and aggregating it with other information taken from public or private sources—such as by cross-referencing databases and collecting the history of an individual's interactions or information shared in the past. Needless to say, an individual has the right to change their ideas and modify their identity over time. But moreover, the information—insofar as it is personal (which it does not cease to be by virtue of its disclosure online[29])—must be able to be protected on account of

---

28 "Irrespective of the fact that the petitioner's information on his Twitter account and his tweets can be openly viewed by the public, the respondent [the presidency] was not authorized to use it as if it were public data and on that basis draw up the list of influencers in which it included the act, since it is clear that what determined its inclusion and the qualifier of 'negative' was precisely his political ideology, which was reflected in his social media interactions" (Corte Suprema de Justicia 2020).

29 "Not all data found in a public database, in mass media or the internet, are public by this fact alone" (Superintendencia de Industria y Comercio 2022); "personal data found in publicly accessible sites such as social media or the internet are not rendered public by that fact alone" (ibid.).

its connection with different fundamental rights, including the rights to privacy and to the protection of personal data in digital environments, which are, in turn, instrumental to the exercise of other rights that are of both individual and collective interest, such as the right to freedom of expression.

It is true that the expectation of online privacy, or the possibility of controlling the use of one's personal information on the internet, faces serious challenges in a variety of scenarios. And discussions on the scope of these rights stretch far beyond the debates concerning the deployment of state intelligence on the internet and social media.

It is also true that, given the complexity of these challenges, the ones posed by intelligence activities seem to play a marginal role. Awareness of this complexity serves to focus the debate and contextualize our proposal—especially because we are discussing a state activity that should be conducted under constitutional limits and in accordance with the rule of law, which is characterized by institutional dynamics that have been built over the course of decades by democratic systems.

4.2 Our Proposal: Regulation Based on Similar Cases

Social Media Intelligence

When reflecting on the legal limits of online intelligence activities, we would do well to borrow from the limitations typically imposed on two prominent practices in Colombian intelligence activities: passive monitoring of the electromagnetic spectrum and the interception of communications. We propose that social media intelligence be treated as an active form of online monitoring that warrants a protection status similar to that granted to the interception of communications.

The Colombian legal framework distinguishes between passive spectrum monitoring and the interception of telecommunications. Passive monitoring of the electromagnetic spectrum involves the indeterminate, abstract, and temporally limited tracking of the invisible highway through which com-

munications travel and is directed at identifying threats to the array of social goods that intelligence seeks to protect (Corte Constitucional, Sentencias C-540 de 2012 and C-570 de 2010).

When passive spectrum monitoring seeks to cross over to the profiling of a person to listen to their communications with others, we are dealing with the interception of communications that, because of its impact on privacy, may proceed only with a warrant. Its outputs are subject to review by a national judge tasked with guaranteeing the legality of the procedures and the protection of fundamental rights, including the right to privacy of the affected persons (Leyes 906 de 2004 and 1621 de 2013). Because it implies a concrete limitation on the sphere of the right to privacy of a specific individual, the intelligence agencies do not have the powers to do so.

Active monitoring on social media involves both reading and collecting information associated with the interactions of a single individual on a given social media channel. This type of monitoring is neither impersonal nor abstract; it is aimed at profiling a person. Insofar as it seeks to answer the question of "who is who," it intentionally aims to diagnose their personality and behavior (past and present), to reveal their interactions and networks of contacts, and to characterize their social habits and even their political, religious, or ideological views. All of this is done with an eye toward aggregating this information with other information that comes from public and private sources, with the ultimate goal of drawing potentially risk-laden conclusions for the individual being monitored.

As a result, actively monitoring social media has a highly invasive potential, equivalent to the invasion of privacy arising from the interception of communications. Now, if social media channels seek, in general, to serve as spaces for social interaction among individuals, who, in the process of such interaction, exchange all types of information about themselves (which may include private and sensitive personal data), why not ensure that these environments have guarantees that are similar to those that apply to the exchange of private communications? Moreover, why would it be considered reasonable to establish a

distinction in terms of privacy guarantees based on the medium in which information circulates and the medium through which it is obtained?

In other words, if studying individuals through their interactions on social media generates the same result as activities to intercept communications—that is, profiling through monitoring—in principle there would be no grounds to grant to intelligence activities on social media weaker guarantees than those that apply to the infringement of privacy in the context of activities to intercept communications. Both tasks have a similar impact on the private lives of individuals.

Of course, accepting this position would mean reforming intelligence activities to submit their collection measures for review by an independent body, which provides a valuable opportunity to strengthen the country's legislation on intelligence through the incorporation of United Nations best practices for this field. In this regard, Special Rapporteur Scheinin notes that "it is good practice for intrusive collection measures to be authorized by an institution that is independent of the intelligence services, i.e., a politically accountable member of the executive or a (quasi) judicial body," or by a judicial body, which is "independent of the intelligence process and therefore best placed to conduct an independent and impartial assessment of an application to use intrusive collection powers" (2010, para. 35).

Bestowing the guarantees of external and independent supervision, similar to those applicable to the interception of communications, to the active monitoring of social media would ensure, among other things, (i) a review of the relevance, adequacy, purpose, and necessity of the information (private and sensitive) sought from social media for the purpose of profiling a person; (ii) a review of the justification of the measure, which should be duly substantiated; and (iii) an assessment of what a reasonable period would be for such monitoring. For each of these tasks, existing jurisprudence on the interception of communications may provide elements that can be used to build good standards.

With the adoption of this type of measure, the tasks of

investigating and deciding on the relevance of the collection of information that is highly invasive of privacy would fall to two different bodies, in contrast to the current state of affairs, in which the superior of the person issuing the order for an intelligence mission is responsible for verifying the compatibility of that measure, along with any limitations it might represent for the rights of the individual in question.

It would also allow the affected individual to exercise their right to due process by, for example, requesting the exclusion of their personal and sensitive information, either because it is no longer relevant (e.g., in cases when an intelligence investigation has already concluded or has been archived), because it has been obtained illegally or unlawfully, or because it is based on discriminatory criteria—such as being a member of a political party, a human rights defender, or a journalist who is critical of the administration.

Moreover, when intelligence information is to be used as a guiding criterion in judicial proceedings, it should be possible to notify the affected individual that their personal information has been gathered in the course of intelligence activities, which would entitle them to exercise the right to access and publicly challenge the personal information in question.

Intelligence Gathered Elsewhere on the Internet

The intelligence gathered elsewhere on the internet—that is, outside of social media—warrants a separate discussion. Here, we should consider the impact of the intelligence gathering that is deployed on the most superficial layer for users, known as the content layer.[30] This layer comprises all other online platforms, services, and applications where user-generated content and information circulate and justifies a differentiated analysis, which

30 There are types of intelligence that are deployed on the physical or infrastructure layer of the internet. Due to its particularities and its potential to be highly invasive of individuals' communications, this type of intelligence warrants a separate approach from the one we propose for the intelligence that takes place on the content, services, and applications layer.

already poses a challenge in the regulation of online intelligence in an ecosystem of intermediaries that is constantly mutating.

This distinction, however, is important. Observations on the monitoring of social media cannot be extended to the monitoring of instant messaging services, for example. This is so not only because the two types of services are platforms with different information architecture but also because the dissemination of information among their respective users serves dissimilar communicative purposes, for which privacy expectations may vary.

For example, the expectation of privacy vis-à-vis the state is much greater when it comes to communications exchanged through private messaging services than with regard to messages posted on social media for a more or less open audience, depending on the social media channel in question.

Obviously, technological guarantees such as encryption preclude the state's passive monitoring of messages sent through certain instant messaging services. In cases such as this, authorities' access to messages (and the metadata associated with them) should conform to specific rules that, at the very least, provide for judicial review or authorization mechanisms.

Efforts beyond Regulation

All that said, it may not be advisable to completely inhibit the deployment of intelligence gathering on the internet aimed at dealing with threats to national security that take place online. To this end, an additional call for reflection is in order considering the potential for the duplication of capabilities insofar as the intelligence deployed on the internet is also in the hands of entities that specialize in cybersecurity issues. Both serve a preventive purpose, but what are the limits or boundaries of each?

According to a document issued by the National Council for Economic and Social Policy entitled "National Policy on Trust and Digital Security," there is not enough interaction, coordination, harmonization, or cohesion between cybersecurity entities, on the one hand, and traditional intelligence entities that conduct work online (including the Armed Forces and

the National Police), on the other. This prohibits an understanding of the objectives pursued by each group when containing threats in the digital environment (CONPES 2020).

Such a lack of interaction and cohesion is not a minor issue among entities exercising intelligence powers with the same preventative purpose. In fact, we asked the Cyber Emergency Response Group, which is a member of the group of organizations charged with protecting national digital security, if it deployed monitoring or profiling activities on the basis of the online activity of internet and social media users, to which it replied that it did not.[31]

However, as we have seen thus far, "traditional" intelligence entities that have more recently shifted their efforts to the internet are doing so in the context of their role of protecting national security, regardless of the environment in which a threat arises, multiplies, or circulates; so how do these two groups of entities coordinate with one another in the digital world? Moreover, how should we understand the scope of action of internet intelligence and cybersecurity and cyber-patrolling activities? The influx of state security forces on the internet and social media warrants a comprehensive approach that draws attention to a potential hyper-surveillance scenario of internet users' activity, which has not been fully explored to date.

In the face of this scenario of growing hyper-surveillance, which hails from multiple origins, a logical response would be to strengthen the mechanisms for ensuring the transparency of intelligence agencies. In this regard, the good practices outlined by United Nations Special Rapporteur Scheinin call for informing "the general public about the type of personal data kept by an intelligence service; this includes information on the type and scope of personal data that may be retained, as well as permissible grounds for the retention of personal information by an intelligence service" (2010, para. 37). Along with these efforts, it is necessary to insist on the declassification and purging of intelligence archives, which should be conducted in an independent manner and with the oversight of civil society organizations.

31 See file no. 221042369 (June 17, 2022).

Finally, the discussion on the limits placed on intelligence gathering on the internet and social media goes beyond the analysis of how to exploit a medium on which personal information that is declared of interest circulates and that affects, among other things, the right to privacy. This is a discussion that requires addressing a much larger picture involving diverse actors, capabilities, and technologies. Yet a comprehensive view of the problem should not lose sight of the fact that individuals are at the heart of the matter, as is the need to guarantee and protect their rights, regardless of the setting involved.

VOLVER AL CONTENIDO

5. Recommendations

Improving the regulation of intelligence is a task with multiple priorities. In addition to traditional calls to strengthen mechanisms for judicial, disciplinary, political, and internal monitoring and control of intelligence activities, to define institutions' competencies and powers, and to ensure transparency in the acquisition of mass surveillance technologies and the purging of intelligence archives, there is a need to better address the internet and social media.

The internet and social media are much more than a strategic medium for obtaining context information. For the individuals who use them, they are a space to meet, socialize, and exchange with others. Exploiting these arenas for intelligence purposes should take into account the uses and purposes currently served by the internet, which increasingly tend toward the growing digitization of life and are expected to lead to greater and more diverse flows of information about individuals. As a first step in addressing some of the problems identified in this research, we propose the following recommendations:

For Congress

→ Regulate the right to data protection vis-á-vis intelligence activities on the internet and social media. In terms of the exception introduced by the Personal Data Protection Law of 2012 and the silence of

the Intelligence Law of 2013 on the matter, Congress cannot continue to ignore the relevance and urgency of activating legal controls regarding the personal information that is collected and processed for intelligence purposes.

→ Delimit the scope within which intelligence agencies may gather public personal information held in databases managed by the state. In addition, specify the rules on the collection of personal and sensitive information through sustained monitoring on the internet and social media.

→ Advance the activation of the political control entrusted to the congressional Intelligence and Counterintelligence Commission; the work of this commission is essential to ensure the transparency of this activity and to demand the delivery of information whose access is denied to citizens. Its work should question, among other things, how the internet and social media are exploited, what digital technologies are available and deployed for this task, and how data protection centers are working to ensure that existing guarantees are respected.

For Intelligence Agencies

→ Internally regulate practices on the use of the internet and social media within the framework of intelligence agencies' duties. Ensure that such regulations include precise instructions for intelligence investigators on the types of personal information that may be extracted from the internet and social media, the criteria that should guide the collection of context information about individuals and their contacts, and how such information will be processed based on the nature of the personal data (public, private, or sensitive), among other things.

→ Strengthen the processes for training intelligence agents on the use of the internet and social media.

In particular, raise agents' awareness about the value of the internet as an environment for circulating and exchanging ideas and opinions. It is a space where the same privacy guarantees that apply offline should also apply and where the presence or activity of individuals should not be understood as an automatic waiver of their right to the protection of their personal information.

→ Ensure the institutional uptake of Law 1712 and the consistent application of its content. Confidentiality should be exceptional and based on more than just the fear that disclosing information about, for example, the type of data collected from the internet and social media could be "used by the enemy" to counteract the state's efforts to protect national security.

For the Rest of the National Government

→ Delineate the roles, scope, and reach of internet intelligence activities vis-à-vis cybersecurity activities so that the convergence of the multiple public entities involved in protecting national security online does not result in a redundancy of functions leading to the multilayered surveillance of internet users.

→ Make progress in the purging of intelligence files. While this mechanism does not grant individuals direct control over their personal information contained in intelligence databases, it allows others to ensure that information that has exhausted its cycle or value or was collected illegally is finally discarded. In addition, the purge should be undertaken with the participation of civil society organizations and independent bodies that can monitor this process, as has been requested by Dejusticia in the past.

For Academia and Civil Society

→ Advance the analysis of the effects that intelligence

on the internet and social media has on the right to the protection of private life and its instrumental nature for the exercise of other rights, such as freedom of expression. Such an analysis should revisit old axioms, such as the impossibility of exercising procedures to control personal data in the hands of intelligence agencies.

→ Question the standards of protection for fundamental rights in the context of the internet, which should not be dependent on the medium in which the information circulates but rather be determined according to the potential impact of using such information for purposes not foreseen by the individual.

→ Specifically, thought should be given to the desirable guarantees in light of the impact on the right to privacy of gathering information (public, private, or sensitive) that was published on the internet during a person's exercise of freedom of expression, of aggregating this information with other sources of public and private information, and of profiling by monitoring online activity to support or test hypotheses that have potentially negative impacts on the individuals concerned.

VOLVER AL CONTENIDO

References

Akhgar, B. 2016. "OSINT as an Integral Part of the National Security Apparatus." In *Open Source Intelligence Investigation: From Strategy to Implementation*, edited by B. Akhgar, P. S. Bayerl, and F. Sampson. Springer International Publishing.

Bruneau, T. C., and S. C. Boraz. 2007. "Intelligence Reform: Balancing Democracy and Effectiveness." In *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness*, edited by T. C. Bruneau and S. C. Boraz. University of Texas Press.

Congreso de la República. 2004. *Ley 906 por la cual se expide el Código de Procedimiento Penal.* http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004.html

———. 2012. *Ley 1581 por la cual se dictan disposiciones generales para la protección de datos personales*. http://ww.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

———. 2013. *Ley 1621 por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones.* https://www.funcionpublica.gov.co/eva/ gestornormativo/norma.php?i=52706

Consejo Nacional de Política Económica y Social (CONPES). 2020. *Política Nacional de Confianza y Seguridad Digital (3995).* https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Corte Constitucional. Sentencia C-1147 de 2001. https://www.corteconstitucional.gov.co/Relatoria/2001/C-1147-01.htm

———. Sentencia T-729 de 2002.

https://www.corteconstitucional.gov.co/relatoria/2002/t-729-02.htm

———. Sentencia C-570 de 2010. https://www.corteconstitucional.gov.co/RELATORIA/2010/C-570-10.htm

———. Sentencia T-708 de 2008. https://www.corteconstitucional.gov.co/relatoria/2008/T-708-08.htm

———. Sentencia C-913 of 2010. https://www.corteconstitucional.gov.co/RELATORIA/2010/C-913-10.htm

———. Sentencia C-540 de 2012. https://www.corteconstitucional.gov.co/relatoria/2012/c-540-12.htm

Corte Suprema de Justicia. 2020. Sentencia STP9319-2020. https://vlex.com.co/vid/sentencia-corte-supremajusticia-851632638

Departamento Administrativo de Presidencia. 2011. *Decreto 4179 por el cual se crea un Departamento Administrativo y se establece su objetivo, funciones y estructura*. https://www.funcionpublica.gov.co/ eva/gestornormativo/norma.php?i=44666

———. 2014. *Decreto 857 por el cual se reglamenta la Ley Estatutaria 1621 del 17 de abril de 2013, "por medio de la cual se expiden normas para fortalecer el marco legal que permite a los organismos, que*

llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con su misión constitucional y legal, y se dictan otras disposiciones." https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=57315#0

Dirección General, Policía Nacional. 2014. *Resolución 01446 por la cual se establece el Manual de Inteligencia y Contrainteligencia para la Policía Nacional*.

Dirección de Inteligencia Policial. 2022, June 10. Response to access to information request, filing DIPOL-ASJUD-13.

———. 2022, September 5. Response to access to information request, filing GS-2022-028515/DIPOL-ASJUD-13.

DNI. 2022, June 14. Response to access to information request, filing 2-2022-139C.

———. 2022, August 29. Response to access to information request, filing 2-2022-2113.

Ejército Nacional. 2016. *Resolución 01886 por la cual se aprueba el Manual Fundamental del Ejército MFE 2-0 Inteligencia*.

———. 2017. *Resolución 01869 por la cual se aprueba la actualización del Manual Fundamental del Ejército MFE 2-0.*

El País. 2020. "Chuzadas en Colombia, un fenómeno ilegal que parece no tener fin." May 6. https://www.elpais.com.co/ colombia/chuzadas-en-un-fenomeno-ilegal-que-parece-no-tener-fin.html

Fundación para la Libertad de Prensa. 2020. "Páginas para la libertad de expresión." *Revista de la Fundación para la Libertad de Prensa (FLIP)* 4.

Gibson, H. 2016. "Acquisition and Preparation of Data for OSINT Investigations." In *Open Source Intelligence Investigation: From Strategy to Implementation*, edited by B. Akhgar, P. S. Bayerl, and F. Sampson. Springer International Publishing.

Hassan, N.A. 2019. "Gathering Evidence from OSINT Sources." *Digital Forensics Basics*. Apress.

Internet Rights & Principles Coalition. 2015. *The Charter of Human Rights and Principles for the Internet.* https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf

Marzell, L. 2016. "OSINT as Part of the Strategic National Security Landscape." In *Open Source Intelligence Investigation: From Strategy to Implementation*, edited by B. Akhgar, P. S. Bayerl, and F. Sampson. Springer International Publishing.

Miller, B. 2018. "Open Source Intelligence (OSINT): An Oxymoron?" *International Journal of Intelligence and Counter Intelligence* 31(4): 702–19.

Ministerio de Defensa. 2015. *Decreto 1070 por el cual se expide el Decreto Único Reglamentario del Sector Administrativo de Defensa*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=76837

Ministerio de las Tecnologías de la Información y las Comunicaciones. 2022, June 17. Response to access to information request, file no. 221042369.

Omand, D. 2017. "Social Media Intelligence." In *The Palgrave Handbook of Security, Risk and Intelligence*, edited by R. Dover, H. Dylan, and M. Goodman. Springer.

Omand, D., Bartlett, J., and Miller, C. 2012. "Introducing Social Media Intelligence." *Intelligence and National Security* 27(6): 801–23.

Pallaris, C. 2008. "Open Source Intelligence: A Strategic Enabler of National Security." *CSS Analyses in Security Policy* 3(32): 1–3.

Privacy International. 2020. *Is Your Local Authority Looking at Your Facebook Likes?* https://privacyinternational.org/sites/default/files/2020-05/Is%20Your%20Local%20Authority%20Looking%20at%20your%20Facebook%20Likes_%20May2020_0.pdf

Policía Nacional, Dirección de Investigación Criminal e Interpol. 2021, August 24. Response to access to information request, file no. GS-2021-108176-DIJIN-CECIP 1.10.

———. 2021, June 30. Response to access to information request, file no. GS-2021-DIJIN-CECIP-1.10.

Policía Nacional, Escuela de Inteligencia y Contrainteligencia "Teniente Coronel Javier Antonio Uribe Uribe." 2022. Response to access to information request, file no. GS-2022-001408/DIRECGUSAP-29.25.

Revista Semana. 2020a, May 1. "Las carpetas secretas." https://www.semana.com/nacion/articulo/espionaje-del-ejercitonacional-las-carpetas-secretas-investigacion-semana/667616/

———. 2020b, January 12. "Chuzadas sin cuartel." https://www.semana.com/nacion/articulo/chuzadas-por-que-seretiro-el-general-nicacio-martinez-del-ejercito/647810/

Scheinin, M. 2010. *Compilation of Good Practices on Legal and Institutional Frameworks and Measures That Ensure Respect for Human Rights by Intelligence Agencies while Countering Terrorism, including on Their Oversight*. UN Doc. A/HRC/14/46. United Nations Human Rights Council.

Steele, D. R. 2007. "Open Source Intelligence." In *Handbook of Intelligence Studies*, edited by L. K. Johnson. Routledge.

Superintendencia de Industria y Comercio. 2020, December 15. Radicación 20-423123.

———. 2022, July 13. Radicación 22-212677.

State intelligence gathering has long since shifted to the internet and social media. This poses additional risks to the exercise of the right to privacy, which already faces serious obstacles due to harmful practices exercised by other actors.

In this report, we explore this subject by drawing on the "Secret Dossiers" case published in 2020 by *Semana* magazine, which shows how the Colombian state exploits social media and the internet in order to monitor and profile individuals.

Our analysis warns that the safeguards present in existing legislation are rather sparse and that intelligence agencies' desire to self-regulate on the issue of open source intelligence is almost nonexistent despite these agencies' surprising clarity about the data on the internet and the social media that interest them.

Our proposal begins by affirming the importance of the right to privacy in the digital world, including vis-à-vis the state. We believe that, in the discussion on desirable limits, the insights that have emerged regarding the passive monitoring of the electromagnetic spectrum and the interception of communications offer valuable lessons for better addressing the impact of online intelligence.

We hope that this report will help advance discussion on a topic whose ethical and legal challenges deserve the attention of internet users and the legal community.