Unseen Followers

A first approach to government use of Open-source intelligence (OSINT) and Social media intelligence (SOCMINT)

por los Derechos Civiles

Asociación por los Derechos Civiles

With the support of

Initially published in October 2018. English version published in October 2019.
https://adc.org.ar

This work was done as part of a project financed by the International Development Research Centre (IDRC). It is published under a Creative Commons Attribution-NonCommercial-ShareAlike license.

To see a copy of this license, visit: https://creativecommons.org/licenses/byncsa/2.5/.

The document *Unseen Followers* is for public dissemination and has no commercial purpose.

Table of contents

Invisible Followers

A first approach to government use of Open-source intelligence (OSINT) and Social media intelligence (SOCMINT)*

I. Introduction

It is estimated that every 60 seconds on the internet, people send 187 million emails; perform 3.7 million search queries; send 38 million messages through WhatsApp; post 481 thousand tweets; watch 4.3 million videos on YouTube; download 375 thousand applications; share 174 thousand photos on Instagram and spend 862 thousand dollars on online purchases. If we multiply these figures by hours, days, months and years, we will get a clear picture of the significance the internet has gained throughout the last decade.[1]

In a context of innovation and technological advancement, the advent of web iterations brought about a number of services that have permeated our daily lives, changing the way we communicate with our beloved ones, do business, share information, look for and consume entertainment or learn something new.

With the arrival of platforms that fostered an increasing social web, a new era of services was brought to life, accompanied by changes in business models and in behavioral patterns regarding content consumption and online interaction among people.

In parallel, due to the need to investigate unlawful actions occurring both online and offline, more emphasis is being placed on the relationships between people and technology in view of the omnipresence of technology in modern society, especially when it comes to the activities they carry out and the services they use on the internet. Currently, people use online profiles in social networks as a window to their thoughts, behavior, preferences, routines, intimate and professional relationships. In essence, some of the most essential characteristics that are core aspects of their identities.

The purpose of this report is to contribute to a discussion which is currently neither on the

---

* This document was drafted by **Leandro Ucciferri**, lawyer, public policy analyst and researcher of the Digital Area, at Asociación por los Derechos Civiles (ADC). https://adc.org.ar

[1] What Happens in an Internet Minute in 2018?", Visual Capitalist, May 2018, available at: http://www.visualcapitalist.com/internet-minute-2018/

public agenda nor in the democratic forums where public policies are created. Under the pretense of the free availability and advertising of information shared on the internet, States all over the world have silently taken advantage of its exploitation for the most varied purposes. This document is not meant to give a comprehensive account of all the intrinsic particularities of this matter, but to trigger and promote a well-deserved public debate, especially when it comes to the protection of fundamental rights.

In this sense, in the following chapters, we will conduct a preliminary research by analyzing the growing use of research techniques of information in open data sources and social networks by various Argentine government agencies, focusing primarily from the viewpoint of crime investigation.

In the **second section**, we explain the definition of Open-Source Intelligence (OSINT) and Social Media Intelligence (SOCMINT); their growing popularity in the digital age and their potential impact on fundamental rights. We devote the **third section** to a case study chosen for our research: the use of these techniques for public security purposes and for combating crime. We will focus on the analysis of some relevant cases of the last two years and the greater role assigned to the Ministry of Security together with other law enforcement agencies. Finally, in the **fourth section**, we provide a number of preliminary recommendations for the enhancement of public policies respectful of human rights perspectives.

II. Investigation in open sources: internet and social networks. What are OSINT and SOCMINT?

The investigation of information from open data sources, known as Open-source intelligence (OSINT), refers to the practice of using a set of techniques and technologies to collect publicly available information[2], such as texts, images, videos, audios and even geospatial data. Once said data is given a purpose within a specific context, and is assigned to an actionable task, it turns into intelligence.

OSINT can be traced back to the beginnings of the development of intelligence services around the world. As technological development created new ways of communicating and sharing information, open source investigations adapted to the new circumstances. In this sense, the advent of the press, radio, television and the internet marked significant milestones as they increased the amount of data and information, making them available to an incommensurable number of people around the globe.

The development of the internet marked a before and after regarding the possibility to

[2] Publicly available refers to information that any person can access without the need of special access credentials of any type, as opposed to information which is protected by, for example, user and password.

exploit information using OSINT tools. This explains how the internet quickly leveled with the rest of the intelligence collection disciplines. Even though open sources such as newspapers, magazines, radio and television programs or academic works can be easily accessed at a low cost, with the advent of the internet, and in particular with the expansion of the web, the limits hindering the growth of OSINT, one of the main investigation disciplines, began to whittle away. However, this situation has some disadvantages too. The amount of information created per minute on the internet can be a double-edged sword. Accessing practically every repository of information produced by humankind can be overwhelming, discouraging and intimidating. On top of that, it requires a great amount of resources –time, human and economic or a combination thereof– to be effectively processed and analyzed.[3]

In this context, it is urgent to promote a public debate regarding the impact these investigation techniques may have on fundamental rights, particularly on the right to privacy and freedom of speech. The way we use the internet can be exploited to the benefit of others and this may have consequences in our daily lives. Security forces and state agencies have taken advantage of the fact that the internet is open and public to reproduce a *status quo* which allows them to access information available therein without accounting for it. Thus, people are led to believe that there's no expectation of privacy on what is shared and published on the internet.

Thanks to this *status quo*, a lax conception has become popular regarding the scope of OSINT, particularly with respect to the inclusion in this discipline of data collected from social networks. However, it is necessary to draw a sharp line to describe the particularities of each discipline.

The analysis of social networks or Social Media Intelligence (SOCMINT) basically refers to the collection and processing of data from different platforms (Twitter, Instagram, Facebook, YouTube, Snapchat, to name some of the most popular ones) where users post their opinions, photos, videos and participate in conversations or just read about international news.

The use of SOCMINT for investigation purposes may involve several techniques, such as: manual revision of published content; revision of specific user searches, hashtags, groups, among others; revision of activities or types of contents published by users; the use of scraping tools to extract content from a webpage; and even the systematization of one or many of these techniques through different types of software.

A clear distinction has to be made between OSINT and SOCMINT when it comes to their use by the state, especially for crime prevention and investigation. This is due to the fact that

[3] "The Strategic Use of Open-Source Information", John Gannon, Intelligence Community Perspective, available at: https://www.cia.gov/library/readingroom/docs/DOC_0006122487.pdf More information in: https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source- intelligence.html

social network platforms challenge a rigid conception between public and private, since, most of them, are governed by private companies that have their own rules of the game, such as their terms and conditions and privacy policies.

However, the affirmation that there should be no privacy expectation when it comes to using a social network is inaccurate and, on top of that, it stifles the debate we must promote as a society on regulations involving the use of these techniques by the State and the private sector.

It is no news we live in a hyper-connected society. In the last decade, there has been an exponential yet silent fusion between our online and offline lives. With each technological advance and new product launched into the market, we have so naturalized the way we interact with our devices that they have become an extension of our body and mind. By the same token, our interactions with other people have gone digital too, so that nowadays it is common to learn about what our relatives and friends are up to just by looking at their posts in social networks.

Social sciences began to explore this phenomenon in an attempt to analyze human behavior in the digital era from a theoretical framework. Spanish sociologist Manuel Castells has referred to our social structure in this era of information as "network society", as it is governed by centralized networks existing under a new paradigm of time and space not bound by geographical limits.

The analysis of this phenomenon cannot fail to consider the economic aspect though. The main technological companies, most of which are based in Silicon Valley, California, have developed a digital economy that has shaped interactions between people and technology. According to philosopher Byung-Chul Han, people expose themselves voluntarily and cheerfully and their exposure has become a systemic coercion fed by the very same platforms. Han refers to this new phenomenon as "exhibition society", where everything has to be shown in order to exist. This results in the creation of an exposure value, which aims to attract attention or likes in the world of social networks, as each subject becomes its own object of publicity.[4]

The digital market created and developed by companies such as Facebook and Google bases its business models on the massive exploitation of data obtained from their users in order to monetize people's attention and sell advertising. This is what Han terms "the panoptic market", where surveillance capitalism imposes an obligatory exposure and the excess of visualization is turned into merchandise. Meanwhile, the inhabitants of the digital panoptic[5] think they are free.

---

[4] The Transparency Society (Transparenzgesellschaft), Byung-Chul Han, Herder, 2013.

[5] The term was coined by Jeremy Bentham, an English philosopher from the utilitarian movement, at the end of the 18th century. It refers to the structural design of a prison where all prisoners can be observed simultaneously in their individual cells, without them knowing whether they are actually being observed by prison guards, which produces the sensation of being under constant surveillance. The concept was later studied by French philosopher Michel Foucault in his work "Discipline and punish" (1975).

Having provided an analysis on how social networks are designed so that people will grant access to their private lives, we should move on to two other aspects closely connected with SOCMINT: first, its usefulness and reliability and, in secondly, its impact on privacy.

In the first place, what people express online, and in social networks in particular, does not necessarily coincide with what they actually think. In the field of psychology, the online disinhibition effect is related to people's behavior when they interact in the digital world as opposed to their in-person interactions.

People may display substantially different behaviors whether in the digital or face-to-face world. Some of the factors that contribute to creating this effect are: the feeling of safety derived from the ideas of distance and temporality; the similarity or monotony of profiles, which results in the minimization of status and authority; and a dissociative imagination that leads them to believe that what happens online is fictitious, separate and apart from the real world.[6]

Social network platforms introduce a layer of complexity to the study of online expressions, given that certain tools and functions allow for messages to reverberate outside their own social circles, making it trickier to grasp the reach of those messages.

In the second place, the control users have over what personal information is published in social networks (in other words, their so-called information self-determination) does not always respond to their voluntary or predetermined choice. On the contrary, there are various factors involved, such as:

- metadata contained in posts (geolocation, time zone, language, devices used, etc.)[7];
- posts made by other users that may contain personal information;
- privacy settings, which are updated as platforms evolve. These settings do not offer protection by default, as publicity is often the norm. On the other hand, the addition of new functions to the platform often involves the collection of new types of data, causing a new learning curve.

In this sense, the privacy expectation a person may have in a given social network is directly related to the knowledge they have on how that platform works.

European case law determined that people are entitled to an expectation of privacy even in public spaces. This was upheld by the European Court of Human Rights (ECHR) in the case Peck v. United Kingdom (2003), where the Court acknowledged the existence of a zone of

[6] "The Online Disinhibition Effect", Suler, J. (2004). CyberPsychology and Behavior, 7, 321-326. Available at: https://pdfs.semanticscholar.org/c70a/ae3be9d370ca1520db5edb2b326e3c2f91b0.pdf

[7] For example, a single tweet of 140 characters may contain metadata representing 20 times the size of the posting. A detailed description of the metadata found in tweets and how to analyze them can be found in the following link: https://blog.0day.rocks/you-will-be-surprised-by-what-your-tweets- may-reveal-about-you-and-your-habits-3bc907688bc8

interaction of a person with others, even in a public context, which may fall within the scope of "private life" and therefore be entitled to protection.[8]

The analysis of online profiles does not only apply to comments, opinions and other types of expressions posted in web platforms. As we briefly mentioned in the previous paragraphs, posts are often accompanied by another type of equally valuable information which is overlooked on many occasions. When data concerning geolocation, people's feelings behind their posts, contact networks interacting with a person's profile or with specific content are collected daily, weekly, monthly or yearly, and analyzed altogether, it can give us an incredibly detailed notion of a person's habits and customs throughout their lives.[9]

The systematic analysis performed by state agencies of social network activities is not too far off from a reality where every conversation taking place in urban public spaces are recorded via microphones.

Apart from the clear interference in people's privacy, monitoring and analyzing information posted in social networks have clear effects on freedom of speech. People adjust or modify their behavior when they know or feel, even if remotely possible, that they are being observed and judged. The use of SOCMINT techniques creates a chilling effect regarding people's behavior on the internet. As a result, citizens tend to increase their self-censorship levels.[10]

---

[8] In the case of Peck v. United Kingdom, the applicant complained about a local council passing footage recorded by the close circuit television (CCTV) to the media, which led to the publication and broadcasting of images showing Peck in a suicide attempt. The local authority running the CCTV system, the Brentwood Borough Council, had passed images to the media in an attempt to present the system as a highly effective tool of both crime deterrence and detection. The Independent Television Commission (ITC) and the Broadcasting Standards Commission (BSC) considered that the masking was inadequate as many of his neighbors, colleagues, friends and family who watched the programs recognized the applicant. The European Court of Human Rights determined that the passing of images to the media resulted in a breach of article 8 of the European Convention. The Court emphasized that even though the applicant was on a public street, he was not participating in a public event and neither was he a public figure, adding that the release of images was unnecessary in a democratic society. Case of Peck v. United Kingdom, European Court of Human Rights, January 2003, http://merlin.obs.coe.int/iris/2003/6/article2.en.html More information available in: "CCTV and Human Rights: the Fish and the Bicycle? An Examination of Peck V. United Kingdom (2003) 36 E.H.R.R. 41", Caoilfhionn Gallagher, Surveillance & Society, 2004, http://www.surveillance-and-society.org/articles2(2)/humanrights.pdf

[9] Regarding this argument, we should refer to the common law "Mosaic Theory" developed by Orin Kerr, based on which the exhaustive collection and aggregation of data resulting from surveillance activity, even when such data may seem harmless, provides more detailed knowledge compared to the analysis of individual pieces. Hence, during a given time period, it is possible to create a mosaic of habits, relations and more details regarding the private lives of monitored people. This represents a violation of the Fourth Amendment of the U.S. Constitution. "The Mosaic Theory of the Fourth Amendment", Orin Kerr, 111 MICH. L. REV. 311, 312 (2012): https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1079&context=mlr; "How Long is Too Long? The 4th Amendment and The Mosaic Theory", 2014: http://lawandlibertyblog.com/nyujll/2014/6/3/how-long-is-too- long-the-4th-amendment-and-the-mosaic-theory

[10] For a suggested article on the chilling effects of surveillance involving online freedom of expression please read:

1. A global issue with real consequences in our fundamental rights

The number of cases reported in the last years shows the global magnitude of this issue. Far from addressing this problem, many governments around the world have turned to the implementation of OSINT and SOCMINT techniques for their work, reflecting a new reality for modern digital life: our internet activity, especially social network communications, is being stared at lustfully in terms of its potential for the investigation of illegal behavior.

In Boston, United States, the American Civil Liberties Union (ACLU) showed concern over racial discrimination on the part of the police department after it used a tool to monitor social networks unfairly focusing on people using the hashtag #MuslimLivesMatter on Twitter.[11] This kind of behavior displayed by the American government had been previously reported in connection with the movement #BlackLivesMatter.[12]

In Canada, several government agencies and departments proactively use tools and other practices to monitor different social networks,[13] and have even helped develop software to facilitate the collection and processing of information.[14]

In Egypt, by mid 2014, the government was said to have developed a plan to acquire technologies in order to monitor social networks with the excuse that it needed to identify "security hazards" and "persons representing a danger on society" by collecting and analyzing opinions that constitute "destructive ideas". In the copy of the call for tenders leaked to the media, the Ministry of Interior lays out what it means by "destructive ideas", through an extensive list, including concepts such as: blasphemy and skepticism in religions; taking statements out of context; pornography and lack of morality; sarcasm, among other situations.[15]

By mid 2018, the Egyptian president ratified a law granting the Supreme Council for Media

---

"Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study", Jon Penney, Internet Policy Review, May 27, 2017, available at: https://ssrn.com/abstract=2959611

[11] "Boston police's social media surveillance unfairly targeted Muslims, ACLU says", Alanna Durkin Richer, Associated Press / Boston Globe, February 7, 2018, available at: https://www.bostonglobe.com/metro/2018/02/07/boston-police-social-media-surveillance-unfairly-targeted-muslims-aclusays/9JUpzPmy8Tsr5RLxvCm61M/story.html

[12] "The Government Is Watching #BlackLivesMatter, And It's Not Okay", Nusrat Choudhury, ACLU, August 4, 2015, available at: https://www.aclu.org/blog/racial-justice/government-watching-blacklivesmatter-and-its-not-okay

[13] "The Canadian Government Told Us It's Down With Social Media Monitoring", Ben Makuch, Motherboard, November 14, 2014, available at: https://motherboard.vice.com/en_us/article/vvbpb9/the-canadian-government- told-us-its-down-with-social-media-monitoring

[14] "Monitoring your memes: The government has helped develop software to monitor your social media for threats", Justin Ling. VICE News, March 9, 2017, available at https://www.vice.com/en_ca/article/nedxez/the-canadian-government-developed-software-to-monitor-your-social-media-for-threats

[15] "Egyptian Government Wants Surveillance System To Monitor 'Destructive Ideas' On Social Networks", Privacy International, June 13, 2014, available at: https://privacyinternational.org/blog/1252/egyptian-government- wants-surveillance-system-monitor-destructive-ideas-social-networks

Regulations the power to place people with more than 5,000 followers on social media or with a personal blog or website under supervision. In addition, the Council was authorized to suspend or block any personal account which publishes or broadcasts fake news or anything inciting violating the law, violence in general or hatred.[16]

In Venezuela, since 2014, at least two dozen people have reportedly been imprisoned, generally without due process, for anti-government opinions expressed in their Twitter accounts and for messages containing financial information such as the dollar exchange rate.[17]

In Chile, the federal security force, the *Carabineros*, reportedly conducts "cyber surveillance" activities in social networks with an equipment especially designed for this task.[18]

III. "Cyber-patrolling" the internet: The role of open source investigation in Argentina

The use of techniques and tools of investigation in open sources began to permeate the State at least a decade ago. Throughout these years, many government agencies have explored the use of different platforms and technologies which allow them to exploit data and information published on the internet to pursue their own purposes and goals. In this sense, there are various initiatives in the fields of taxation, education and public security, just to name the ones that have gained more public importance.

At the beginning of 2007, the former director of the Fiscal Agency of the Province of Buenos Aires (ARBA) announced the incursion of the Agency into fiscal intelligence tasks via satellite images. The official told the newspaper La Nación that they had been working for four years on the digitalization of blueprints of plots and properties of the provincial territory to cross check the information against the satellite images obtained from Google Earth Pro (a license which initially cost the yearly sum of 400 dollars before Google started offering it for free in 2015). This would facilitate the work of inspectors sent later on to the field, to corroborate the information previously collected.[19]

In June 2008, ARBA made public the results of a four-year investigation that aimed to identify tax evaders in the agricultural field. To verify tax returns lodged by landholders

[16] "Egypt's President el-Sissi ratifies law to monitor social media users", DW, September 2, 2018, available at: https://p.dw.com/p/34Aak

[17] "Encarcelado por tuitear", Luis Carlos Díaz, Derechos Digitales, June 18, 2018, available at: https://www.derechosdigitales.org/12273/encarcelado-por-tuitear/

[18] "El desconocido 'ciberpatrullaje' de Carabineros en las redes sociales", Víctor Rivera, La Tercera, August 28 2018, available at: https://www.latercera.com/nacional/noticia/desconocido-ciberpatrullaje-carabineros-las-redes-sociales/299027/

[19] "Montoya busca evasores con el Google", La Nación, February 21, 2007, available at: https://www.lanacion.com.ar/885329-montoya-busca-evasores-con-el-google

owning lands greater than 50 hectares, ARBA's intelligence team used satellite images to analyze the potential existence of constructions and improvements made to such lands, which allowed them to detect, for example, undeclared crops.[20]

Likewise, the Municipal Revenue Agency of the city of Mar del Plata announced, in 2012, operations where, for the purposes of detecting inconsistencies in tax returns, it crosschecked information of the municipality's database with ARBA's blueprints and Google Maps' updated satellite images.[21]

ARBA's incursion into the exploitation of satellite images evolved into the "Integrated Strategic Satellite Monitoring" program. It was launched in 2014 and allows the agency to crosscheck information between 18 satellites and various databases containing tax information[22]. It also entered into an agreement with the National Commission of Spatial Activities (CONAE) and started using satellites with better capabilities to capture more accurate images.[23]

By mid 2016, in the Province of Buenos Aires, the government made a request for tender inviting private suppliers to "implement an analytical observatory, updated in real time, to deal with the different educational issues (…) presented by various actors of the education community, including the State and its public policies, through social networks", with an estimated budget of $1,597,200 pesos.[24]

In early September 2017, the Ministry of Economics and Finance of the Autonomous City of Buenos Aires authorized a public tender for the procurement of an "Analytics Solution for Structured Data and Big Data" for a total of $17.500.000 pesos, in order to equip the Government Administration of Public Revenue (AGIP) with tools to identify and manage risks resulting in potential tax evasion, citing as an example in the specifications the possibility to predict taxpayers' behavior based on the monitoring of their tweets and the analysis of conversations that may signal their intention to commit fraud.[25]

Two weeks later, the tender opening procedure was postponed after "multiple queries and requests for a deferral".[26] Finally, at the end of December 2017, the tender process was cancelled,[27] "in order to contemplate the needs of the General Office of Statistics and Censuses and guarantee a greater participation". Based on the Official Gazette, "Avanzit

---

[20] "Con satélites, detectaron 10.000 silos sin declarar en Buenos Aires", Clarín, June 22, 2008, available at: https://www.clarin.com/ediciones-anteriores/satelites-detectaron-10000-silos-declarar-buenos- aires_0_HyKze0nATKe.html

[21] "ARBA y la Municipalidad detectan grandes empresas y constructores evasores", La Capital, July 25, 2012, available at: http://www.lacapitalmdp.com/noticias/La-Ciudad/2012/07/25/225280.htm?ref=ar

[22] "MESI: Arba optimiza el monitoreo satelital", ARBA, https://bit.ly/2z14U7w

[23] "Tecnología satelital para combatir la evasión", ARBA: https://bit.ly/2q9ct83

[24] Private Tender N° 9/16, Official Gazette of the Province of Buenos Aires, July 11, 2016, available at: http://www.gob.gba.gov.ar/Bole/pdfs/2016-07-11/OFICIAL2016-07-111467923140.pdf

[25] Public Tender 8618-1261-LPU17, pages 184 and 185, available at: https://bit.ly/2qb6dNg

[26] Official Gazette, page 202, available at: https://bit.ly/2PRWrdV

[27] Official Gazette, City of Buenos Aires, page 247, available at: https://bit.ly/2PjfGA3

Tecnología S.A."[28], "Consenit S.A."[29] and "Grupo Net S.A."[30] had submitted an offer.

1. Anything you tweet may be held against you

We can now go deeper into the field of public security to analyze in detail some of the main events that took place in this domain in the last two years, after the public administration changed. We would also like to consider the new trends that may continue to develop in the near future in this respect.

The arrival of a new president to the Executive after the end-of-year presidential elections of 2015 meant a radical turn in the public policies promoted by the State. The new administration, which was empowered by the electoral success at a national level, in the province of Buenos Aires and in the City of Buenos Aires, promoted a new kind of relationship between the State and technology. It fostered the idea of modernity not only in the way politics is done, but also in terms of how citizens interact with state agencies.

Between 2016 and 2017, amid sudden changes in economic and social policies including the non-renewal of employment contracts of public administration employees, a series of cases involving several social network users came under the spotlight. Users became the target of legal investigations after being accused of different crimes involving the publication of opinions on their accounts.

In May 2016, a woman was indicted on criminal threats under Article 149 bis of the National Criminal Code[31], which carries a penalty of 6 months to 2 years imprisonment (aggravated in the case of anonymous threats), together with the crime of discriminatory acts under Article 3 of Law 23.592[32], which involves "individuals who use any means to incite hatred against or persecution of a person or group of people on the grounds of race, religion, nationality or political inclinations". The latter carries a penalty of 1 month to 3 years imprisonment.[33]

The indictment resulted from tweets posted in early March 2016 by an individual who threatened the then recently elected President, Mauricio Macri and his family, in particular his minor daughter. The judge, Ariel Lijo, established that "a great number of web users were alarmed by those postings, which went viral in many virtual outlets".[34] When the

---

[28] www.avanzit.com.ar

[29] www.consenit.com

[30] www.gruponet.com.ar

[31] The complete version of the updated National Criminal Code is available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm

[32] The complete version of Law 25.592 is available at: https://bit.ly/2rcZdRP

[33] "El juez Lijo procesó a una mujer por amenazar a Mauricio Macri y a su familia", Legal Information Center, May 23, 2016, available at: http://cij.gov.ar/nota-21585-El-juez-Lijo-proces-a-una-mujer-por-amenazar-a- Mauricio-Macri-y-a-su familia.html

[34] National Judicial Power, Federal Criminal and Correctional Court No. 4, 2398/2016, Page 2.

threats were posted, they received 8 retweets and 2 likes only. However, they were quickly captured by many pro-government users, who passed the messages to thousands of other users in the platform, mainly through screenshots.[35] One may just look up on Twitter the username of the person who made the threats in order to see the exchange of messages, the information shared and the tone of the tweets.[36]

This was one of the first cases that made the term "cyber-patrolling" popular. It was defined by the judge Lijo as the kind of patrolling made "by police officers who specialize in crime prevention, contraventions and summary offences taking place on the internet". As per the decision of the court, the Cybercrime Division of the City of Buenos Aires conducted "a search in open sources on the internet". Likewise, the Police carried out a research on Facebook in order to find the profile of the person using the Twitter account.

Before continuing with the overview of the case, it is worth discussing another increasingly common phenomenon seen in the last few years that can be identified in the tweets made by users as a result of the published threats: the dissemination of personal information for intimidating purposes or the so-called "*escrache*", a subtype of public shaming.

After the threats received media attention, many Twitter users began to disseminate personal data of the woman who would be later indicted, such as her ID number and "CUIT" [Unique Tax Identification Code], her address, full name and date of birth. In this way, users went from being simple participants in a conversation or exchange to police officers, prosecutors and judges. This situation was assessed by the judge for the sole purpose of confirming the crime charges filed against the Twitter user on account of the fact that she created quite a commotion by inciting violence in a conversation taking place in the social network. Notwithstanding the aforementioned, the judge seized the chance to remark that if the person had only expressed criticism towards the government's actions -even using a hostile or aggravating tone- the postings would have been considered to be part of the exercise of the freedom of speech and thus afforded constitutional protection.

As per the court decision, when making her statement, the accused declared that her broadside had been the result of losing her job in the National Ministry of Social Development. However, the judge considered that the user's threats constituted a crime as she posted several messages from a Twitter account containing false personal information (name, avatar and biography), all of which exceeded the concept of "broadside".

In section VII of the court decision, the judge analyzed the impact that his decision could have on the right to freedom of speech. Firstly, he determined that the Twitter user's messages constituted "expressions of hatred" from a legal standpoint and were therefore prohibited by the different human right treaties. Secondly, the judge pondered the potential consequences of the chilling effect, acknowledging that it may end up being an internalized censorship mechanism that affects society as a whole.

---

[35] There is an example available in: https://bit.ly/2qbn5Dk (Accessed on September 13, 2018)

[36] See for example: https://twitter.com/search?f=tweets&vertical=default&q=%40lamarikaos&src=typd

The reasoning of the judge was that "the sanction imposed on the accused will not lead those participating in any democratic debate to restrict, consciously or unconsciously, their constitutionally protected opinions for fear of a similar penalty".[37] The judge explained that this was due to the fact that the case in point revolved around "expressively prohibited" declarations.

However, there is another aspect involving the potential chilling effect that may affect the freedom of speech and therefore result in self-censorship. This aspect was omitted by the judge in his analysis probably because it was not directly linked to the subject matter of the case –the threats and expressions of hatred posted. It concerns the very issue that we strive to understand in this report. The action of "cyber-patrolling" social networks and the internet in general may negatively affect the way we use the internet, either to communicate, exchange ideas or find information, to name a few basic uses. Internet activities may be undermined by the use of tools, technologies and practices based on policies with little or no transparency both in terms of scope and accountability.

In the following months, more legal cases were brought to the court as a result of threats made to public officials in social networks. In December 2016, a man was prosecuted for posting threats against the president and vice-president, the minister of Security of the Nation and the governor of the Province of Buenos Aires.[38] Finally the case was brought to court in May 2017 with the man being indicted on the crimes of anonymous threats, public intimidation and propaganda justifying or inciting racial or religious discrimination (articles 45, 55, 149 bis and 211 of the Criminal Code and article 3 of Law 23.592).[39] Similarly, a woman was prosecuted in July 2018 for explicit threats against various officials of the Executive and Judicial powers made in September 2016. The indictment was similar to those analyzed in the previous cases.[40] In this last one, the tweet that triggered the case only had 6 likes,[41] while the second tweet received 8 retweets and 10 likes[42] by the time this report was done.

Based on the aforementioned cases and the analysis done of the impact these investigation techniques may have on people's rights, we can highlight some questions that arise: In terms of public intimidation crimes, how is the relevance of online declarations measured? Does it suffice to consider the number of retweets, favs, likes or interactions? By the same token, if declarations are made by one person with only a few followers or contacts –as it occurred with most of the cases mentioned in this chapter–, is it the same for that person

---

[37] National Judicial Power, Federal Criminal and Correctional Court No. 4, 2398/2016, Page 34.

[38] "Detuvieron a un hombre que amenazó a Mauricio Macri por Twitter", Infobae, December 20, 2016, available at: https://www.infobae.com/politica/2016/12/20/detuvieron-a-un-hombre-que-amenazo-a-mauricio-macri- por-twitter/

[39] "Elevan a juicio oral una causa por intimidación y amenazas contra Mauricio Macri", Legal Information Center, May 16, 2017, available at: http://cij.gov.ar/nota-25920-Elevan-a-juicio-oral-una-causa-por-intimidaci-n- y-amenazas-contra-Mauricio-Macri.html

[40] https://web.archive.org/web/20180914195133/https:/twitter.com/Albor_Adrian/status/1023962054678532096

[41] Accessed on September 14, 2018, available at: https://bit.ly/2CDjh5k

[42] Accessed on September 14, 2018, available at: https://bit.ly/2PVfu7o

to make such declarations in a park or square? Should the number and type of followers be analyzed to verify whether these accounts belong to real people as opposed to spam profiles or bots?

In regards to the last question, we may argue that the threats investigated in many of the legal cases received greater attention once they were identified by government supporters, who passed these threats among their own contacts in order to repudiate them. Otherwise, the tweets may have gone unnoticed.

If we had to pin down the moment when "cyber patrolling" took on a more prominent role in public conversations, that would be between end of January and beginning of February 2017. Despite the fact the State seemed to be more pro-active in its fight against crime, back at that point Security minister Patricia Bullrich's twitter account was compromised by a phishing[43] attack along with many other institutional emails. An electronic communication was sent to her institutional email disguised as an official message from the Embassy of Bolivia. The occurrence was quickly made public after Twitter users first saw the messages posted from Bullrich's account and then spread the news along with details of the alleged illegal access.[44]

Not until mid-February of that year were two people detained for being the alleged perpetrators of phishing and for having illegally accessed the minister's Twitter account and the institutional emails of the Ministry of Security. In March, the judge of the lower court filed formal charges against one of the detainees. The court decision referred to the role of the Technology Crimes Division of the Federal Police in the "cyber patrolling" tasks carried out by corporal Jorge Landajo.

According to the description provided by the judge, the report of the Police that conducted the "cyber patrolling" tasks was based on the investigation of search engines, Twitter and Instagram. As part of the investigation, the corporal of the Federal Police recovered many tweets posted by a well-known expert of the technical community who spread the news in his personal Twitter account.[45]

The events involving the minister's Twitter account and the institutional emails of the Ministry of Security were used as a justification for the new strategy adopted by federal forces to combat crime. Just three months after the incident, the minister announced the re-launching of the Federal Police, highlighting that the police would go from police department to investigation unit; that employees would go from police officers to detectives and that territorial procedures would turn into intelligent and unexpected operations. She added that it would embark on "cyber patrolling" tasks in order to find

[43] Phishing refers to a social engineering technique generally used to obtain confidential information. For more information please visit: https://www.segu-info.com.ar/malware/phishing.htm

[44] Tweets recovered on January 26, 2017 are available in: https://bit.ly/2yyLDL3

[45] "Patricia Bullrich y el 'ciberpatrullaje'", Javier Smaldone, March 9, 2017, available at: https://blog.smaldone.com.ar/2017/03/09/patricia-bullrich-y-el-ciberpatrullaje/

criminal groups on the internet.[46]

Ten days prior to the Eleventh Ministerial Conference of the World Trade Organization (WTO), hosted in Buenos Aires, a new event would put Argentina under the international spotlight. Sixty four persons, most of whom were human rights advocates and activists, members of twenty one civil society organizations, were informed by the WTO that, despite having been accepted and duly authorized to participate in the Conference, the Argentine security authorities had denied them access to the event and they even risked being denied access to the country.[47]

In a press release of early December 2017, the Ministry of Foreign Affairs and Worship backed this decision, establishing that some of the shortlisted participants "had made an explicit call for violent demonstrations through social networks, expressing their intention to bring about chaos and intimidation".[48] The news soon aroused controversy in social networks and the international media.[49] Amid deportations and conflicts with the admittance of foreign participants to the Conference, it remained to be seen how the Argentine government had arrived at the conclusion communicated by the Ministry, as the selection of unauthorized organizations seemed to follow no logic.

Public discussions were flooded with doubts. Why did they decide to monitor social networks to look for declarations related to the Conference? What were the tasks carried out by the Argentinean government to find the declarations of violence? Which kind of expressions did they consider capable of bringing about "chaos and intimidation" through social networks?

In order to find an answer to these and other questions, we made two requests for access to public information before the Ministry of Security and the Ministry of Foreign Affairs.

Both ministries categorically denied each one of the questions raised regarding the background checks and their involvement in the accreditation process of participants. Even though the Ministry issued a notice to the Federal Intelligence Agency (AFI) for it to answer

---

[46] "Se relanzó la Policía Federal con su nueva función de 'ciberpatrullaje'", Clarín, April 18, 2017, available at: https://www.clarin.com/policiales/relanzo-policia-federal-nueva-funcion-ciberpatrullaje_0_B1KKunQ0x.html

[47] "Preocupa la negación de acreditaciones a organizaciones de la sociedad civil a la reunión de OMC en Buenos Aires", ADC, December 1, 2017, available at: https://adcdigital.org.ar/2017/12/01/preocupa-la-negacion- acreditaciones-organizaciones-la-sociedad-civil-la-reunion-omc-buenos-aires/

[48] "Sobre la acreditación de ONG's a la Conferencia Ministerial de la OMC en Buenos Aires", Information for the Press N°: 558/17, Ministry of Foreign Affairs and Worship, December 2, 2017, available at: https://cancilleria.gob.ar/es/actualidad/comunicados/sobre-la-acreditacion-de-ongs-la-conferencia-ministerial-de-la-omc-en-buenos

[49] See: "Argentina blocks some activists from attending WTO meeting", Reuters, 30 de noviembre de 2017, available at: https://www.reuters.com/article/us-argentina-wto-protest/argentina-blocks-some-activists-from-attending- wto-meeting-idUSKBN1DU39V

"Fury as Argentina blacklists WTO attendees over 'calls for violence'", The Guardian, December 11, 2017, available at: https://www.theguardian.com/world/2017/dec/11/argentina-social-media-ban-world-trade-organisation-conference

"Argentina bans activists from WTO meeting", Financial Times, November 30, 2017, available at: https://www.ft.com/content/9dc1a640-d5ff-11e7-8c9a-d9c0a5c8d5c9

the request, no reply was received by the time this report was finished. However, in regards to the request made by the Center of Legal and Social Studies (CELS) when the event took place, the AFI declared that it had not been involved in the accreditation of participants.[50]

State agencies displayed an elusive behavior when requested to provide details of the incident. They did not account for the intelligence tasks carried out to conclude that declarations of violence had been made in social networks by members of the unauthorized organizations. The Ministry of Foreign Affairs as well as the Ministry of Security and the Federal Intelligence Agency were elusive in their answers too, only allowing for speculations as to their involvement in the organization of the Conference. They failed to clarify what expressions set the alarm among security agencies working in the event or what criteria were used to classify them as expressions of violence. They also failed to determine who conducted the investigations on social networks and which platforms they mostly targeted.

2. National Ministry of Security and federal security forces

In view of the latest events taking place in the last two years and in order to shed light on the way the Ministry of Security and its federal forces conduct investigations in open sources and social networks, we made a request for access to public information in early July 2018. The aim was to go deeper into the information provided exclusively by the media.

The request centered on two important aspects. On the one hand, it focused on the court cases initiated on account of declarations investigated on the internet in order to elucidate: protocols followed when carrying out these tasks, if any; the number of cases investigated thus far in connection with online declarations; the criteria followed to determine the legal basis of the investigations; the way data is collected and analyzed; the kind of authorizations requested to conduct online investigations; the type of training given to personnel performing investigation tasks; and the methods, techniques and technological tools used for online investigations.

On the other hand, we requested information on the concept of "cyber patrolling" as used by the Ministry and federal forces in order to clarify the type of tasks and activities involved, the applicable protocols and the training given to the personnel performing these tasks.

Initially, the first reply given by the Ministry in early August 2018 did not fully address the questions raised in the 13 items of our request. On the contrary, the Ministry simply provided a brief and generic description of the functions of the "Cybercrime Investigation Directorate", created in March 2018; a literal transcription of Resolution 234/2016, which comprises the General Response Protocol of the Police and Security Forces in the

[50] EX -2018-9330179-APN-AAIP_Reclamo CELS C/Ministerio de Relaciones Exteriores y Culto y Agencia Federal de Inteligencia https://www.argentina.gob.ar/sites/default/files/rs-2018-20-apn-aaip.pdf

Investigation and Evidence Collection Process of Cybercrimes; and finally, a closing statement establishing that "with regard to the use of open sources, general and not particular policing policies are applied."

Dissatisfied with such a basic reply, we decided to file a claim with the Agency of Access to Public Information (AAIP), which issued its final resolution in mid-September 2018. Once the claim was filed, the AAIP requested the Ministry to provide any and all relevant documentation in reply to the request made by ADC. The Ministry sent the Agency three documents providing additional information and notified the Argentine Federal Police and the Airport Security Police.

In the new reply, the Ministry establishes they are working on the implementation of indicators to produce statistics and measure the performance of the Cybercrime Investigation Directorate. In addition, they confirm the implementation of policing policies to detect crimes in social networks. They have still been unable to report on the estimated number of investigated online cases since minister Bullrich took power, arguing the Directorate is not old enough.

Regarding the distinction made between OSINT and SOCMINT as two concepts that must be addressed separately, the Ministry stated they do not conduct investigation tasks. However, in another section of the reply, they affirm they use open sources to conduct their investigations, which the ministry understands to be "accessible to any citizen". Likewise, even though the Directorate denies performing forensic IT tasks under the General Response Protocol, security federal forces are on their way to implement said protocol for "cyber patrolling" activities in the evidence collection process.

When asked to provide a definition of "cyber-patrolling", the Ministry stated that the Agency has not come up with a definition as of yet, but is analyzing it from a technical and legal perspective. However, the document issued by the Technology Crimes Division of the Federal Police does define "cyber patrolling" as "the colloquial way of referring to information searches in public and open sources related to cyberspace".

"Cyber patrolling" tasks are conducted manually, without any type of software or automated process, by conducting searches in search engines and using the available tools provided for free on the internet. However, said tools were not disclosed in the reply received by ADC.

The General Office of Complex Crime Investigation and the Technology Crime Division of the Argentine Federal Police confirmed that online investigations, in other words "cyber patrolling" activities, are initiated upon a court order requesting said activities. The Cybercrime Investigation Unit of the Ministry of Security has "investigation powers established under the Administrative Decision that enacted it, which means it can appear before the court and request the different means of evidence established in procedural codes."

Finally, the trainings for the security forces personnel conducting online investigations are

provided by officials and agents of said forces, the Ministry of Security and international agencies such as Interpol. Neither the Argentine Federal Police nor the Ministry provided more details as to the training of their employees. The Ministry added that the information and materials used for training is confidential pursuant to article 8 of Law 27.275.

3. Police of the City of Buenos Aires

The situation of the Police of the City of Buenos Aires (formerly Metropolitan Police) is not far from the reality faced by the Ministry of Security and the federal forces. In an interview with ADC, a person close to the Police provided details on the role of the force in the investigation of crimes in the digital domain. For professional reasons, the interviewee asked that their identity be kept confidential, which is why they are identified here as "P.I." (protected identity).[51]

Even though the City Police often used investigation techniques in open sources, they are not yet being fully exploited. This is mainly due to a matter of training and resources. **P.I.**: "The lack of exploitation has to do with the lack of trained personnel, data science, database analysts and experts. This has to do with the investment needed to build the infrastructure required for a good analysis."

"They use a single concept which is analysis or investigation of information in open sources of data. This is the term you may find in summary proceedings or legal cases. Legally and technically speaking, it saves them from using the English term in a legal document."

P.I.: "Open source intelligence encompasses all of the information which is public and was obtained through mechanisms that do not violate the applicable laws. For example, it is one thing if I look for someone's Facebook page using their phone number and find it, but it is not the same if I find a database leak by someone who hacked LinkedIn, look for the username and password of a given person, and use that information to obtain intelligence. It is indeed an open source, because the information was there. But the source of the information can be challenged. If the defense [attorney] catches on to this, they can file a motion to annul the entire proceedings."

For the purpose of legal proceedings, the investigation of open sources is seen as just another investigation stage.

P.I.: "Scenario 1: An officer of the court calls you and tells you there is a warrant for you to pick up. You go to the courthouse, ask to see the case file, sit down with the clerk, the judge or the prosecutor –depending on how familiar you are with them–, and they tell you: 'look, we are investigating this drug trafficking case, it is connected with this, and we have this information." Sometimes they ask you what can be done and sometimes they already have an idea of what they need: 'we need you to check these Facebook profiles or these

[51] Interview with ADC on July 16, 2018 in the City of Buenos Aires, Argentina.

email accounts and conduct an open source analysis.' For that they give you a warrant, which you use to begin a Police investigation and start completing all of the associated tasks. You distribute the tasks among the members of the team, draft the reports, prepare everything and then go to the courthouse and submit what you have found. If that is all you are asked to do, then the investigation is closed and legal proceedings commence. Otherwise, the initial exploratory investigation is further developed, always with the support of one arm of the judicature."

Once this stage is over, a report is drafted and the case continues. **P.I.**: "This (the result of the investigation) becomes part of the case file. You close the investigation stage, submit your findings to the court and that is it. That information is gone. The Police only keeps a summary stating 'Investigation X; Case X; X time.' They keep no copy of the report, which is submitted to the court, but they do keep a copy of the receipt issued by the court."

The other type of open source investigation is the one in which the Police takes a proactive role in the prosecution of a crime. **P.I.**: "[In this case] you start with a series of selectors[52] linked [for example] to the stealing of auto parts. If you find something, you go before the court and, in this scenario, you take the case to them. If they say yes, you get a warrant and commence the investigation. Otherwise that is it."

In the case of major public events, such as the Ninth WTO Ministerial Conference, the Youth Olympic Games or the upcoming G20 Summit, the situation changes. According to **P.I.**: "there is a series of actions that are carried out to determine whether someone is planning to commit a crime."

P.I.: "The process is automated. Generally, you take some tools and scrape different media (social media, webpages, blogs, forums, etc.) using a series of keywords. That is the starting point. The entire content is scrapped and transferred to a database, which is then transformed into a graphic report which allows you to tell [for example] what the most common hashtag was. Once you reach the point in which you can identify an individual user, the process continues by hand. This is done for specific […] events for which there is a history of troubles. Now, for the Police to say 'Ok, let's look for pedophiles' would be impossible."

What happens if the Police needs to track a specific person or group? **P.I.**: "In that case we use an undercover agent. The agent infiltrates an organization and the investigation is conducted independently and confidentially, in direct communication with the judge. Undercover agents are even allowed to commit crimes, provided they do not endanger themselves or commit a felony. [There is also what we call an] enticing or revealing agent, which can be used online, and can enter a site as a passive spectator."

These cases are as follows, **P.I.**: "For example, [they can] entice someone to follow them to

[52] "Selector" is the term used by the Police to refer to the category or type of information used for the investigation. For example: an email address, a phone number, an ID number or the full name of a given person.

see the content of their Twitter or Instagram profile, but they must be authorized to operate [as an undercover, revealing or enticing agent], otherwise they cannot do this. All details are recorded in the case file: 'X profile was created, with X avatar, for such and such purpose,' and all the content generated for that profile must be previously authorized for the specific revealing agent, who must be identified, for a given period of time, which is usually extended, and for a specific purpose. Once the applicable purpose is achieved, the agent must be retired. Logically, the authorization must be granted by a judge. The platform [social network, forum, etc.] is never made aware. It is the main 'enemy,' because it can eliminate the profiles."

The use of OSINT and SOCMINT techniques by the Police is still at a very early stage. **P.I.**: "For methodological reasons, there must be a protocol the Police can follow. As of today there is no such protocol, there is no qualified personnel and there are no tools. For the time being most things are done based on common sense and the use of manual and open-source tools. [It is an] artisanal work of searching, copying and viewing."

4. A brief overview of internet platform statistics

The importance given by governments to information coming from social networks can be measured by looking at the reports published by platforms providing the services.

Nowadays, the publication of transparency reports has become a standard for internet companies. They help analyze the evolution of personal information requests made by government bodies in many countries around the world.

Based on the information provided by Twitter, as table 1 shows, it is evident that the number of requests made by Argentinean State agencies from January 2016 to December 2017 increased compared to the four previous years. However, the company did not provide the requested information in all cases. This may be due to a number of reasons: the specific profile was not identified; the request was excessively general; the user may have claimed the request after being notified or the company may have asked the requester for more contextual information and received no answer, among other situations.[53]

Period	Account information requests	Percentage of requests where some information produced	Accounts specified

[53] A detailed description of personal information requests in Twitter can be found at https://transparency.twitter.com/en/information-requests.html

July – December 2012	2	0 %	13
January – June 2013	2	0 %	2
July – December 2013	1	0 %	1
January – June 2014	7	0 %	8
July – December 2014	3	33 %	4
January – June 2015	3	0 %	3
July – December 2015	4	0 %	14
January – June 2016	18	22 %	33
July – December 2016	76	26 %	87
January – June 2017	57	12 %	64
July – December 2017	80	10 %	100

Likewise, the reports published by Facebook show the same increase in the number of personal information requests made by the Argentine State to the platform. Unlike Twitter, Facebook has a higher percentage of information produced and delivered for each request.[54]

Period	Total Requests	% of Requests Where Some Data Produced
January – June 2013	152	27 %
July – December 2013	278	18.40 %
January – June 2014	254	31.90 %
July – December 2014	482	48.50 %
January – June 2015	568	46.10 %
July – December 2015	892	71.30 %
January – June 2016	829	74 %
July – December 2016	995	75 %
January – June 2017	984	76 %
July – December 2017	1290	80 %

[54] A detailed description of personal information requests in Facebook can be found at: https://transparency.facebook.com/government-data-requests/country/AR

IV. Recommendations

Based on the information presented in this report, we may conclude that the use of OSINT and SOCMINT techniques by state agencies, especially for crime investigations, is a complex issue with many implications.

It is necessary to discuss these techniques in depth before public policies are implemented by the Government for their exploitation. In this sense, the analysis of the techniques should address the protection of fundamental rights such as the rights to privacy, freedom of speech, free assembly and association. It should also address considerations on data protection and the role of the private sector both as the facilitator of the technology used for investigation tasks and of users' information stored in the platforms.

In this sense, we would like to propose the following preliminary recommendations with the view of promoting the discussion, development and enhancement of public policies devoted to the use of OSINT and SOCMINT that are respectful of human rights.

1. The data collected by state institutions must be necessary and proportionate for a legitimate aim. The information shall be stored in databases only when strictly necessary. People must know that the police and other governmental bodies collect their information from open sources and social networks –including inferences made from said data– so that they can fully exercise the rights afforded by the Law on Data Protection (access, rectification, suppression and updating). Any refusal must be duly founded.

2. It is necessary to establish specific protocols with a comprehensive approach to this issue. The use of data by security forces and other state agencies must be clearly defined, transparent and available to the population, so that its necessity and proportionality can be easily assessed. Response criteria should not be subject to interpretations of public officials or members of the security forces only.

3. Said protocols should follow accountability guidelines, including the regular publication of reports with objective statistical information and minimum details such as: number of cases and investigated individuals, plus the duration of the activities; social networks and websites monitored; the tools and methodologies used for each case under investigation. Likewise, the consequences resulting from the violation of any policy must be clearly defined in order to reduce the potential for abuse of surveillance practices.

4. Besides, protocols must provide clear guidelines on how to assess the reliability, veracity and quality of the information that is collected, processed and stored. This

would allow answering questions such as How can we distinguish and identify seemingly illegal declarations from those which in fact are jokes or part of a cultural exchange, or even part of the language that we find on the internet?

5. Finally, the training received by officials, personnel or employees responsible for the implementation of investigation and surveillance techniques must be based on a human rights perspective, especially when it comes to the right to privacy and freedom of speech, as well as the legal data protection framework.


por los Derechos Civiles