

# **The Influence Industry Personal Data in Colombia's 2018 Legislative and Presidential Elections**

researched and written by  
[José Luis Peñarredonda](#)



in partnership with Tactical Technology Collective's  
*Our Data Our Selves* project  
[ourdataourselves.tacticaltech.org](http://ourdataourselves.tacticaltech.org)

June 2018

## Country profile: Colombia

### 1. Basic information

Colombia has almost 50 million inhabitants [1], of which 77% live in urban areas and 23% in rural areas [2]. Its capital, Bogotá, with a population of around 7.9 million people, [3] is the most populated municipality in the country and contains 15.8% of the population.

Colombia's government is divided into three branches of public power (executive, legislative and judicial) and three administrative levels (national, departmental and municipal; see table 1). At present there are 32 departments and 1,122 municipalities. At each of these levels the heads of the executive and legislative branches are elected by popular vote; other mechanisms are in the judicial branch. Departmental and municipal elections are held every four years and the next ones are to be held in 2019. National elections are also held every four years, with one date for the election of the Congress and another for the election of the president.

Table 1: Administrative levels vs. branches of public power in Colombia

	<b>Executive</b>	<b>Legislative</b>
National	Presidency	Congress
Departmental	Government	Assembly
Municipal	Mayoralty	Council

The most recent legislative elections were held on March 11, 2018, and the presidential elections, which involve two rounds, are scheduled for May 27 and June 17, 2018. In addition, extraordinary elections may be held through participation mechanisms like plebiscites or referendums, the most recent of which occurred on October 2, 2016, when Colombians voted against the endorsement of the peace agreements with the FARC.

Congress is divided into two houses: the Senate (upper house), elected from a national constituency with 107 members; and the House of Representatives (lower house), with departmental electoral districts and 171 members. This means that candidates for the Senate are elected by the country as a whole, while each department (plus Bogotá) chooses a proportion of

the candidates of the House of representatives, and this proportion is determined according to its population.

Parties and movements can choose between what are referred to as “open lists” and “closed lists”. For the former, voters choose a candidate from the party’s lists, and for the latter voters merely vote for the party. Most parties choose open lists: in the legislative elections of 2018, five of the 16 parties with registered lists chose to use closed lists. Of those, only the FARC got senators, and only because of the peace agreements signed in 2016: the votes they obtained would not have enabled them to put more people in Congress.

Citizens choose from president and vice president lists; in this election eight lists were registered. The second round only takes place if no list obtains the absolute majority of the votes in the first round (at least one vote more than 50%) and only the two options with the highest numbers of votes in the previous rounds participate in it. The candidates who obtain the most votes are elected president and vice president. After this election, the candidate who came second for presidency gets a seat in the Senate, and the runner-up vice president enters the House of Representatives.

Candidates can only be registered by political parties or movements, or by significant groups of citizens, groups constituted by collecting a higher number of signatures than those needed to make up 3% of the electoral roll (number people eligible to vote). There are currently 13 parties or movements [4], and for the 2018 elections, 69 significant groups of citizens were constituted [5].

In Colombia anyone over 18 can vote except if their political rights have been revoked. Voting is not mandatory, and it is rare that participation in elections exceeds 50% of the electoral roll. In addition, a significant proportion of the votes are usually invalid, usually because the voter fails to fill in the ballot correctly (see table 2).

Table 2: Electoral roll, valid and invalid votes in the last five elections in Colombia.

	<b>Electoral roll (people)</b>	<b>Valid votes (% of electoral roll)</b>	<b>Invalid votes (% of valid votes)</b>
2018 legislative elections*^	36,493,318	17,818,185 (48.82%)	871,444 (4.89%)
2016 referendum^	34,899,945	12,808,858 (37.43%)	170,946 (1.33%)

2015 local elections <sup>+</sup>	33,792,602	19,115,084 (56.56%)	429,216 (2.24%)
2014 second round of presidential elections	32,975,158	15,794,940 (40.65%)	403,405 (2.55%)
2014 first round of presidential elections	32,975,158	12,844,949 (38.95%)	311,655 (2.42%)

Source: National Registry of Civil Status.

\*: Senate elections data.

^: Quick count data.

+ : Mayoral election data

## 2. Digital industry in Colombia

In the last 10 years, the Colombian digital industry has grown considerably. The government measures connectivity in the number of broad-band connections, and Colombia has gone from having 4.6 million in 2011[6] to 28.4 million in 2017. Of these, 22.2 million are cell phone connections. [7]

Economic activity online has also sharply increased over this period. In 2017 Colombians made digital transactions amounting to 51.2 billion (as in million million) pesos (some 184 million dollars); this involved a 24% increase compared to 2016 [8]. Investment in digital advertising grew 30.2% in 2017, reaching 103,445 million pesos (roughly 37.2 million dollars) [9]. However, there are no precise figures on how many content and digital advertising agencies there are in Colombia.

As of yet, there are no statistics on the political digital marketing industry in this country. Unlike other countries, in Colombia there is no list of authorized suppliers for parties and candidates, which makes this analysis difficult. Nevertheless, there is, as we shall see in this report, an established industry that offers these services and many candidates are making use of it.

Colombia is a country with fairly intense social media usage: according to Facebook's figures, this social media platform has more than 26 million users in the country, more than half of the population, and 17 million use it every day. In fact, according to Facebook spokespeople, Facebook is used from 95% of the country's internet connections [10]. Twitter's figures are not as detailed, but its executives have confirmed that Colombia is one of the top 20 countries in the world in

terms of number of twitter users [11]. Despite there being no figures for WhatsApp, to the casual observer's eye it certainly appears to be the most popular app in the country and to be installed on most cell phones; marketing surveys made by technological firms appear to have reached the very same conclusion [12].

## **Political Actors**

Nationally, Colombia usually votes to the right of the political spectrum: left wing positions have carried the stigma related to armed confrontation for decades and continue to do so to this day. Twice president of the republic (2002-2006 and 2006-2010) and founder of the Centro Democrático (Democratic Center) party, the most influential politician in the country is Álvaro Uribe Vélez, who usually defends pro-market economic positions and traditionalist social positions (pro life, pro drug prohibition, etc.). Uribe was the most voted candidate in the parliamentary elections of 2018, and his party won the most seats.

Other parties of the right or center-right that have votes and influence include the Partido Conservador (Conservative Party), Cambio Radical (Radical Change) and the Partido de la Union Nacional (Social Party of National Unity). These parties' alliance brought the current president, Juan Manuel Santos to power in his second term (2014-2018). In his first term he was supported by Uribe and in his second he defeated the Centro Democrático candidate Óscar Iván Zuluaga. In general, all these parties adopt pro-market positions, although there are some small nuances in their positions, especially on social issues, as some right-wing economic politicians have slightly more progressive positions than others.

The Verde (Green) and the Liberal Party are located in the center. The former was consolidated on the basis of charismatic leadership in the form of Senator Claudia López and Antanas Mockus the former presidential candidate. Although their positions on economic issues cannot be considered left-wing, and they even come close to those of parties that are perceived to be further right on the political spectrum, their positions on social issues are the most progressive of all the political parties. The Liberal Party used to be the most powerful party in Colombia before Uribe entered the political arena and although it currently boasts influential figures at a national level and was part of the alliance that brought Juan Manuel Santos to power, it is not recognized for having a clear political ideology.

The Polo Democrático Alternativo (Alternative Democratic Pole) party, the Decentes list and the FARC are to be found to the left. Polo Democrático is the most institutionalized and the strongest party on the left; it usually supports statist stances and classic left-wing positions for economic questions. Although it is not known for having strong positions on social matters, Polo

Democrático generally leans towards progressive stances. The Decentes list is a conglomerate of several parties and small movements bound together under the presidential candidate Gustavo Petro. Their economic positions are classic left-wing positions, and they adopt progressive stances for social matters. The FARC, who are to participate in politics for the first time, will presumably assume left-wing policies for economic issues, but their positions on social issues are unknown for the time being.

Another important issue to bear in mind is the division and polarization that has been emerging since the referendum on whether to endorse peace agreements with the FARC. Colombia was divided in two: those who supported the agreements and those who rejected them. Even though, at least on paper, most political parties were in the first group (except for Centro Democrático and some conservative sectors) the referendum results reshuffled parties and candidates' stances and serve as a kind of gauge to explain the positions of the candidates for the 2018 electoral process.

On the one hand, what the media called “the ‘no’ coalition” was consolidated, led by those who rejected the agreement. All of them come from right-wing sectors, mostly located in the Centro Democrático and the Partido Conservador; they consider that the agreement does not punish the crimes committed by the FARC fittingly. On the other hand, the “yes” coalition defends the agreements. The entire left supported the yes and so too did some center-right party members (others articulated more ambiguous stances). In many ways, this debate was transferred to the elections of 2018, it clearly divided traditionalist right sectors from the rest of the country and showed the pulling power this issue has among the electorate.

## **Noteworthy cases of digital communication in political campaigns**

### *2016 Referendum*

In the days leading up to the referendum, there was a marked increase in the intensity of the political content circulating on digital platforms in Colombia. The tone of this content betrayed the presence of a fear mongering misinformation strategy based on pre-prepared messages. Social networks and messaging services such as WhatsApp “became spaces for the promotion of anger, fear, disappointment and uncertainty through rampant lies, which reinforced these messages with photographs and videos that circulated silently, whose origin was impossible to establish” [13, p. 467].

In a candid interview, this suspicion was confirmed by the director of the Centro Democrático “no” campaign, Juan Carlos Vélez: “We wanted people to go out to vote *berraca* [angry]” [14]. In this interview Velez offers more data showing the importance of digital platforms for this strategy.

First, he said that it was a very cheap campaign, "with a very high cost-benefit [ratio]", which was possible due to the extensive use of digital tools. And second, he revealed that part of his team was made up of "creatives who are experts in making videos and posting them on social media" [15]. Using a combination of content strategy and psychological manipulation, the "no" sector managed to take advantage of the sheer enormity and virality of social media.

In the wake of this revelation, messaging services (especially WhatsApp) began to gain importance in candidates and political parties' digital strategies. Their use as tools for message dissemination became very common after the success of the "no" campaign. Nevertheless, these revelations highlighted social media and messaging applications' potential for promoting disinformation and large-scale manipulation, which sparked initiatives from journalists, the media, and civil society that countered this type of false content and disinformation campaign [16] [17].

### *The Andrés Sepúlveda and Buggly case*

In February 2014, in midst of the presidential campaign, with Juan Manuel Santos up against Óscar Ivan Zuluaga the Centro Democrático candidate, the Attorney General's Office unexpectedly searched a house in a residential neighborhood of Bogotá, where a hackerspace called Buggly was operating and from which, according to press reports, the FARC peace process was being spied on [18]. The official explanation was that it was a front operation for the Colombian intelligence service that sought to achieve cyber attack and cyber defense capabilities through the local community of computer security experts [19]. This explains why many ethical hackers frequented the site and how Buggly leaders had got integrated into the community [20].

Shortly after this it was learned that the agents who ran the place had links to Andrés Sepúlveda, a social media strategist who had been hired by the Zuluaga campaign to carry out dirty campaign activities. Although it was never possible to verify that Sepúlveda had the capacity to violate the security of computer systems [21], he did surround himself with people who could. An employee of his, Daniel Bajaña, was found guilty of illegally accessing the email account of Francisco Santos, a rival of Zuluaga in the Centro Democrático internal elections. And Sepúlveda, according to the Attorney General's Office, acquired databases for the exclusive use of military intelligence through the agents at Buggly, as well as intelligence information on several members of the FARC. These agents had the tools for electronic espionage and the interception of communications [22].

For spying on the peace process, Sepúlveda was sentenced to 10 years in prison [23]. The Attorney General's Office argued that given the connection between Zuluaga and Sepúlveda, the information purchase was carried out in order to favor the Centro Democrático candidate; although it has not been proven that the campaign made use of these tools. Indeed, it seems even

more plausible that Sepúlveda managed to disseminate content strategically. In an interview he claimed to have the ability to “send 200,000 messages by WhatsApp in an hour [...] send a mention 10 thousand times to a Twitter account” [21], and to have managed to get “people to begin to use rumors I was planting myself” [21].

## 1. Introduction

The widespread use of social networks and digital platforms has resulted in the emergence of a market that seeks to make profit out of data obtained from users or that they themselves provide when using these services. This market has been widely used by the marketing industry, which uses all this information to profile people in order to make internet advertising more effective and personalized.

Since the campaign that took Barack Obama to presidency in 2008, political operators around the world seek to take advantage of these new opportunities and approach citizens in more direct ways. In fact, during this campaign it became evident how “digital media provided opportunities for strategic as well as tactical innovation in electoral contexts where *personal political communication is crucial*”. [24, p. 131]. This has been carried out predominantly (but not exclusively) through social networks such as Facebook or Twitter, although candidates have also acquired increasingly sophisticated private tools.

This study aims to provide an overview of how candidates and parties involved in the 2018 legislative elections in Colombia used these tools. The main research question is: **how much personal information do candidates and parties have about their voters, and how do they use it?** To try to answer this question, we designed a three-stage methodology involving:

- Four semi-structured interviews with people who have information or knowledge about the use of personal data and digital tools in political campaigns.
- An analysis of the digital presence of 48 candidates and 11 political parties. Candidates were chosen either for being the at the top of the Senate lists and House lists of the four most populated jurisdictions in the country, or for having high levels of media recognition and strong digital presences. In this analysis the websites of the candidates and parties and their presence in social networks were examined in search of active data collection mechanisms (registration or mailing forms, for example), passive data collection mechanisms (website activity tracking), and security tools (SSL).

- We made a series of informal inquiries of different actors in order to clarify events or particular circumstances.

Special conditions in the context of Columbia make analyzing the use of personal data in political contests particularly interesting (see the country document): a large part of its population has a presence on social networks, it has a digital industry that offers and exports this type of products and services, and has recent, explicit regulations on the use and processing of personal data.

This report will be structured around the investigations' three main conclusions, each of which will be presented and explained:

- Political parties and candidates have access to Facebook users' information and use it actively.
- A significant proportion of parties and candidates use the web to collect citizens' data, and they do so in ways that put citizens' privacy and rights at risk.
- Politicians access some personal data on citizens through the *dark social*.

### **1. Political parties and candidates have access to Facebook users' information and use it actively.**

Facebook is the most popular and most influential digital platform in Colombia. According to its executives, 95% of internet connections in Colombia are used to access Facebook [10]. It has been calculated that in Bogota, the country's capital, there is a user base of almost 6.5 million people [25], a figure that exceeds the electoral roll (number of people eligible to vote) in the city.

For many of these people, especially the poorest, Facebook is actually the only website they know and use on the internet. For example, a case study conducted by the Karisma Foundation shows how a significant proportion of poor women in Bogotá who use the Internet “have limited their experience to social networks” [26, p. 21] and do not usually follow links outside this platform. This is partly due to the fact that most cell phone operators in the country offer access to Facebook as part of zero-rating billing schemes, so that the data consumed there is not discounted from the client's total balance. This not only reduces the cost of accessing the service, it also discourages users from going on other platforms or accessing the web.

Thus, it comes as no surprise that the priority for the digital operation of political campaigns in Colombia is to communicate through this platform. As one of the interviewees said (2), Facebook “is the biggest contact tool held by a political campaign”. Not only because of its large number of users, but also because of the marketing and audience segmentation tools that the platform offers to digital marketing agencies.

In fact, the study found that it is through these agencies that candidates and political parties use Facebook users' personal data to carry out political marketing operations. As explained by another interviewee (3), "Facebook offers certain public information, and other information that it does not make public, but rather sells to large companies". This non-public information is more extensive and of better quality; it is what allows companies to carry out campaign operations using the segmentation of messages and audiences. This subcontracting model has significant implications when it comes to assigning responsibility for information handling, as we shall explore below.

These techniques are not substantially different to those used in commercial digital advertising. The study found evidence of practices that are widely known and extensively used in digital marketing, such as the design of funnels by a Liberal Party candidate trying to get users to take a certain action (for example to buy something or vote for a candidate) based on a series of interactions with content, or the look alike techniques used by Cambio Radical that search for the audience segment in which a message is most likely to generate an interaction. It was also found that, like in commercial advertising, one criterion to measure the success of these operations is the measurement of campaign results through data analysis tools.

The case of Cambio Radical is interesting because the objective of this operation was to spread the official content of the campaign. The agency handles the creation of content in coordination with the party, defines the audience for each content, and disseminates the appropriate content in the most efficient way possible. To do this they use all the profiling tools they can get hold of. "I collect data on Twitter, I collect data on Facebook, I collect data on Instagram, I collect data on YouTube behavior, I collect data on what the other campaigns say, how much is spent, what it is spent on, what results are obtained. And I collect data on everything in order to know where I'm going. Demographic data, interest data, etc.", said the informant (2).

After the messages are sent, the agency also uses its large volumes of data to measure the effectiveness of the operation, which is done in part by measuring the reactions of users to these messages: "When we download all that information, that's when we generate what's called an insights newsletter, every week we compile an insights newsletter: "the campaign should go this way", "let's not say this again", "this is interesting", the interviewee explained (2).

It's worth mentioning that Cambio Radical is one of the richest and most successful parties in Colombia and has a large budget for this kind of operation. Moreover, the agency in question carries out political digital marketing operations in several countries of Latin America and the Caribbean, so it has a kind of economy of scale which means it can afford sophisticated tools.

In fact, platforms have actively tried to offer some of these tools to parties and candidates. Google held an event in February 2018 in Bogotá; digital communication teams and candidates from political parties were invited and shown the possibilities of some of Google's tools, such as AdWords (the advertising service for keywords) and YouTube. One of the researchers working on this report attended the event and found that teams from various political campaigns were present, which was also revealed by the candidates themselves on their social network profiles<sup>1</sup>.

These new possibilities shape the discourses with which interviewees explain and justify their activity. One of them said (2): "All the reactions that society generates in digital media leave a trace. [...] What we do is summarize all that information and begin to generate strategies based on what people feel, what needs they bring up, what generates resentment, what generates hatred, what they like, what they don't like". And, when asked about how they sell their services to candidates and parties, another of the interviewees (4) answered: "Connecting people, connecting ideas, connecting places, connecting countries ... Connecting, that's the purpose of the Internet".

Specifically, this translates into the possibility, at least in theory, of sending much more specific and effective messages to particular population segments on Facebook, the most efficient channel possible. Mark Zuckerberg's social network not only brings a very significant proportion of the people who vote in Colombia together: it also stores more data about them than most other platforms. This makes it more attractive for those who intend to try to change behaviors, because it makes it possible to look for more flexible, more diverse correlations, which in turn offer more opportunities to elaborate profiles of greater accuracy. Therefore, the promise digital electoral strategists make to their candidates is to personalize their messages and campaigns so that they can convince as many people as possible to vote for a party or a candidate, or even not to vote for other candidates.

It's worth mentioning that digital strategists are aware that this panorama is due, in part, to the fact that users are either unaware that the data they produce on a daily basis are used for these purposes, do not know how to do anything to avoid this, or are uninterested in doing so. As one of the interviewees said (2): "People browse very openly. So, no-one in this country, or I'd say a very small percentage of people would think to use an incognito browser to initiate a browsing session. And at a marketing level, what people do is to take advantage of that and start 'sticking' cookies to you from when you turn on the computer to when you turn it off".

---

<sup>1</sup> On the day of the event, the Liberal Party's presidential candidate Humberto de la Calle confirmed that his team had been there on twitter, though he did not mention the fact that the event had been organized by Google.

The lack of transparency with which commercial advertising segmentation algorithms operate has certain consequences. Not even the actual providers of this kind of service are completely aware of how the algorithms work, the data they use, and the operations they carry out on them. See, for example, an interviewee's response (2) to the question about whether they know which information the look-alike tool uses: "That's the algorithms of the platforms themselves ... Setting up a look-alike strategy involves 'clicking look-alike'. That is 'apple logo + look-alike', and the advertising platforms do it for you".

Of course, this also makes it difficult to know if these techniques are effective without internal campaign data, and there are indications that they sometimes enter into conflict with some campaign realities. One of the interviewees (4) expressed frustration because time and budget limitations prevented them from fully applying their technique to one of the campaigns they were consulting on. They said that there were times when Facebook demographics hindered, rather than promoted, their campaign strategy: "My constant debate with the ad traffickers is that I do not need a public aged 18 to 24[...] I need an older public than that. Because the Colombian voter is, above all, old". While the ad trafficker prefers to 'attack' the younger segments, presumably because they interact with the messages of the campaign more, the electoral realities indicated the need to reach an older segment.

This testimony raises the question of the effects of so-called "digital divides" [27] in democracies in which political communication is mediated by internet platforms. Although Colombia has increased its connectivity, this has not happened uniformly: there has been more of an increase in urban areas than in rural areas, and in middle and upper classes than in lower-income segments [28]. If the electoral debate, the exchange of ideas, and political communications occur mostly online, access to these essential inputs for democratic deliberation will also be unequal in that platforms privilege some segments of the population over others.

In addition, our study found evidence that digital marketing tools are not yet a priority for most candidates and political movements in Colombia, but rather a privilege reserved for those with high budgets or a particular interest in their digital strategy. As explained by one of the interviewees (4), "the other great fear that they [the candidates] have is that they do not feel that digital labor gets converted into votes" and prefer to focus operations on traditional media (press, radio, television) and physical contact.

In any case, all candidates have some kind of digital presence. Of the 59 parties and candidates

analyzed, more than half have a website, and all of them have a presence on a social network (see table 3).<sup>2</sup>

Table 3: The digital presence of the candidates and parties analyzed

<b>Parties analyzed</b>	11		
<b>Candidates analyzed</b>	48		
<b>Digital presence</b>	<b>Active website</b>	<b>Facebook page</b>	<b>Twitter profile</b>
<b>Candidates</b>	21 (44%)	44 (92%)	45 (94%)
<b>Parties</b>	10 (91%)	11 (100%)	11(100%)

\*: Percentage of the 31 websites analyzed (21 belonging to candidates and 10 to parties)

Dissenting stances are also recorded in this study. One of the interviewees (1) expressed their skepticism about the application of these commercial methodologies to political communication, as, according to them, these methodologies are not being used to achieve constructive, two-way political interaction with the voters: “I feel that there needs to be some sort of exercise in hindsight, in listening to what that other is telling me so that I can change, and manage to transform, and not just sell my product”. In the same vein, another of the interviewees (3) said that, for them, “politicians have dedicated themselves to communicating and communicating. But nowadays politics is not done by communicating, it is done by interacting on the internet”.

This difference in criteria reveals a nuance that is worth considering. The acceptance of methodologies coming from commercial advertising is not uncontested among Colombian electoral marketing professionals. The problems found in this study – results that were below expectations, mismatches between the tools’ requirements and the realities of the campaign – are explained by the interviewees in different ways. For instance, there are those who consider that the logic imposed by some of the tools does not fit with the needs of the political activity. Conversely, these problems are also attributed to candidates and parties’ lack of familiarity with these techniques and strategies, and it is believed that the results would be better if these digital tools were used more extensively and competently. In any case, the study found no evidence that the functional and regulatory assumptions that permit the operation of these tools and the

---

<sup>2</sup> Of the candidates analyzed, the only three without a Facebook page have a personal profile on this service. The difference lies in the fact that pages are designed for institutional accounts, while profiles are for individuals.

practice of massive data collection are being questioned. To the contrary all the interviewees recognized personal data collection's importance and utility for obtaining canvassing objectives.

In any case, the political digital marketing industry exists in Colombia thanks to the fact that politically motivated personal data collection on Facebook and other platforms is an everyday reality there, and there is a clear supply and demand for it. The existence of these data silos opens up the possibility of segmenting audiences and messages in ways that were previously impossible. What varies between agencies and strategies is the type of messages sent, and the tactics used to try to make those messages effective. Nowadays, Facebook is the main political and electoral information database in Colombia, and one of the main tools that candidates use to try to convince their potential voters.

**2. A significant proportion of parties and candidates use the web to collect citizens' data, and they do so in ways that put citizens' privacy and rights at risk.**

Parties and candidates also use their websites as tools to collect data on the citizens who visit them. A significant proportion of the studied sites passively record the activity of their users by means of trackers that measure the pages they enter and the links they consult, among other things (see table 3). Furthermore, most of them have a form to collect personal information in an active way; only two of the websites studied contained no tools of this type and both of them were promoting candidates rather than parties (see table 4).

What do the parties and candidates do with the information collected there? Some use this information to deduce the user's identity on social networks and identify them as a possible lead. As one of the interviewees (4) who managed the campaign of a Liberal Party candidate running to be a representative said, "if you enter the website of [name of candidate] and return to Facebook, images of them begin to appear. This is done using software. The software collects the person's information and then, when the person enters, they begin to appear".

Like in commercial marketing, the objective of this strategy is to identify which users have an interest in the candidate and expose them to messages designed so that their interest continues to grow and they start doing small things, such as leaving contact data or following the candidate's Facebook page. Strategists expect that the people who do all these things end up voting for the candidate in question.

In this case, we are talking about a young candidate, who had an environmental and cultural agenda and was trying to get into Congress for the first time (they did not succeed). Although the

informant (4) told us that it was not possible to execute the entire strategy, the candidate in question was said to have been exceptionally interested in this kind of marketing techniques and invested an unusually high proportion of their small budget in digital advertising.

Table 4: Data collection on candidate’s websites

<i>Active data collection method</i>	Subscribing to an email newsletter	Contact form	Donations
<b>Candidates*</b>	7 (37%)	19 (100%)	1 (5%)
<b>Parties*</b>	4 (40%)	8 (80%)	1 (10%)
<i>User trackers</i>	Facebook Connect	Twitter Connect	Other tracking services
<b>Candidates*</b>	8 (38%)	12 (57%)	11 (52%)
<b>Parties*</b>	5 (50%)	7 (70%)	5 (50%)

\*: Percentage of the 31 websites analyzed (21 belonging to candidates and 10 to parties)

Judging by the high prevalence of content forms in the sample analyzed in this study, it is to be expected that this contact information would have been used in an ongoing way to send canvassing information. But the evidence suggests that this does not happen consistently. Although we signed up to 13 SMS forms and 25 email lists, we received only six text messages and 13 emails.

Data collection through websites is a tool that is used across the political spectrum. All the parties analyzed used active data collection tools and/or trackers to collect information passively. Not all the pages studied used both technologies, but the parties all had at least one website where one of these techniques was used.

### ***Insufficient privacy***

Personal data protection regulation in Colombia considers “sensitive data” to be data related to political orientation and political party membership and imposes exceptionally strict obligations regarding its processing. Legally, data subjects must explicitly authorize any processing, and data cannot be given to third parties without their explicit written authorization. Despite this, the practices candidates use to get their hands on and protect the electoral information they obtain from citizens are rather poor.

The security of their websites is below the minimum standards required for the secure transmission and storage of user information and to ensure user privacy. Indeed, many of the candidates who obtain information from citizens neither ask for explicit authorization to store sensitive personal data nor publish their own privacy and personal data protection policies.

Fewer than half the websites analyzed use SSL encryption, a standard protocol which certifies that a website has technologies guaranteeing secure communication between user and server: only 5 out of 10 party websites (50%), and only 9 out of 21 candidate websites (43%). Of those that do use SSL, only two automatically redirect users to a “safe” version of the website.

This exposes website visitors to various security and privacy risks. Firstly, it makes them vulnerable to “injection” code attacks in which a malicious user can run malicious software by typing code into a form, for example, or by intercepting communication between the user and the server hosting the website. Secondly, this oversight makes it possible for a third party who may be examining the user’s web traffic (such as an ISP or an employer) to see that he or she accessed the website in question.

And thirdly, there is a potential case of security malpractice in the system used to receive credit card donations on the website of the only political party to offer this option to its supporters (Centro Democrático). Normally, transactions on websites are made through a “payment gateway”, that is, through an external server responsible for validating the transaction and providing user data security. However, in this case, the credit card information goes directly to the party's servers: meaning that the inputs go into a database with the financial information of the party’s supporters and therefore that it must comply with PCI-DSS security protocols (considered the industry standard for electronic payments).

Although the party states that this data processing is carried out by an external provider, the provider does not indicate that it follows this protocol in its privacy policies or in any other part of its website. In addition, the policies state that the data controller is a civil organization that, as far as we know, has nothing to do with the party.

With regard to the protection of citizens’ personal data, the results of the study reveal a disheartening panorama. Very few candidates report their personal data processing policies on their websites, and although most parties comply with this obligation, not all of them do (see table 3). When we requested a copy of these policies via email from all the sites that did not explicitly state them, we received zero responses.

Table 3: Privacy policies for candidates and parties’ websites

***Is the privacy policy published on the website?***

**Candidates\*** 4 (21%)

**Parties\*** 6 (60%)

\*: Percentage of the 29 websites analyzed (19 belonging to candidates and 10 to parties) which used at least one data collection tool.

There is a debate as to whether or not this behavior infringes on Colombia's data protection regime. On the one hand, it could be understood that when users voluntarily enter their data into a form they are giving implicit permission for these data to be stored and processed, even though at that moment they cannot know what uses they are authorizing, nor who would be responsible in case of abuses or security problems. And yet, on the other hand, it can be argued that if users do not have access to sufficient information, and do not explicitly authorize the processing of these data, their consent is not valid <sup>3</sup>.

Without taking sides in this debate, it would be remiss not to highlight the fact that most candidates and parties put themselves at risk using practices that are not in the best interests of citizens. Under Colombian law, people have the right to keep their political affiliation private, since this can be used as a pretext to discriminate. The fact that an employer, a school or any other authority figure can have access to the activity of a citizen looking for political information online or expressing their sympathy towards a candidate or party not only places their privacy in jeopardy, it also becomes a deterrent against the exercise of political autonomy. Thus, this negligence, regardless of whether or not it is punished by law, has very serious implications when it comes to citizens exercising their freedom of thought and their rights.

It's worth mentioning here that Colombia's personal data protection authority, the Superintendence of Industry and Commerce (SIC as per the acronym in Spanish) already sanctioned a Congress candidate for misuse of personal data online. Sergio Albeiro Guzmán Muñoz, who was hoping for a seat in the House of Representatives in the 2014 legislative elections with the Unión Patriótica party (which in this election is part of the Decentes coalition) was fined 10 million Colombian pesos (around 3,500 US dollars) for communicating information about his campaign using the contact list of an email account he had been assigned when he was a public authority official. Mr. Guzmán Muñoz not only sent canvassing information without the

---

<sup>3</sup> We wish to thank Germán Realpe and Carolina Botero for offering their perspectives on this issue.

authorization of the people who owned those emails; he also thereby disclosed the addresses of some of the recipients [29].

This carelessness is especially worrying when we consider that, as confirmed by several interviewees, these contact lists are everyday input for canvassing activity. One interviewee explained (4) how one candidate used contact networks built up during their previous activity as the director of a foundation: “There are databases there, there is a group of people who work around them, [...] because the person does not start from zero with people who have it. The truth is that the person starts with the influence groups that they created through being in institutions, be they private or public”.

No-one questions that, when carried out in compliance with the law, the use of these lists with personal information on them is legitimate. All politicians have the right to build and increase their electoral capital through activism and contact and volunteer network construction prior to election campaigns and these databases are tools to monitor and capitalize on these interest groups. The problem identified in this study is that, as long as using these lists of personal information for political purposes is the norm, taking the care required by the law to protect the privacy and security of the people whose information is on those lists will be the exception.

### ***Habeas data: from discourse to action***

The laxness of most candidates’ and some political parties’ data protection practices contrasts with the way in which many interviewees talk about the habeas data writ. One of them said (2): “In other countries where we work, the situation is probably much more folksy and their habeas data management is probably not as serious as in Colombia at this time. Using information for something you don’t have the authorization for is an unnecessary risk [...] it’s stupid to get yourself a lawsuit and a fine of 300 million pesos for using an e-mail wrong”

This risk is not run when data collected through social media and other technological platforms is used, as the platforms themselves are responsible for the protection of the data they store. Nevertheless, it is clear that the regulation of personal data in Colombia is perceived as a legal and ethical framework from which political campaigns cannot escape.

On the same vein, there is an awareness of the importance of not using personal data inappropriately, both because of the legal risks and the cost to party and candidate reputations this entails. As one interviewee recounted (1), “you’ll find yourself down the line, a year after the election campaign, getting a huge quantity of spam. Because it turns out that it doesn’t stay within the campaign or within the party, but in the database of the company hired for the mass mailing”.

Another indication of data misuse is the large number of reports social network users made about unsolicited messages, calls, and regular mail that this study was able to identify (see image 1). Moreover, the Electoral Observation Mission (MOE), a Colombian civil society organization that monitors the integrity of elections, received several complaints from citizens about the same irregularity. In some of them, the strategies used several “data points” from the same recipient. For example, calls in which citizens were “reminded” of their polling station came in and they were then invited to vote for a candidate. This requires knowing the person’s name, the number on their citizenship card (their ID card) and their phone number. The arrival of letters addressed to citizen residences complete with their names and surnames was also reported.<sup>4</sup> However, the MOE did not provide details about specific candidates or parties.

Image 1: Complaints about unsolicited messages on election day

---

<sup>4</sup> We wish to thank the Electoral Observation Mission (MOE as per the acronym in Spanish) for this information.



Source: <https://twitter.com/irenerd/status/972651571308843008>

Irenerd: Don't vote for anyone who sends messages via WhatsApp, SMS, calls or emails. They are violating the habeas data writ, they are committing crimes by getting in touch with you.

Kike Gavilán: So, is @muciar Ramirez breaking the law? Because I never authorized anything and I don't know where they got my #, it must have been my operator, Movistar who gave it to them, I guess.

"Find out the proposals of the most experienced candidate in the Gran Consulta por Colombia (center-right primary). Tomorrow, vote for Marta Lucía".

Irenerd: Yes, she is breaking the habeas data writ.

It is impossible to confirm whether all these cases involved actual violations of the regulation on personal data use. Firstly, because it is possible that people had given their authorization without realizing it, in ways that nevertheless complied with the legal requirement. Secondly, because inappropriate data processing can only be investigated if the person concerned files a complaint with the SIC. As we did not receive unsolicited messages in the course of the investigation, we could not carry out that procedure.

Part of the problem is that, as noted in other case studies on privacy policies in Colombia, the language in which authorizations are is still obscure and specialized; often the manner in which the authorization is written allows the data controller to use the data in ways that have nothing to do with the product or service that the data subject tries to access [30].

In addition, the subcontracting model used for most digital political communication strategies in Colombia further extends this ambiguity. Colombian law allows for two types of responsibility in data protection: that of the controller, the one who makes decisions about data processing, and that of the processor, the one who actually does the processing. Often, the controller is the party or the candidate, and the processor is the agency that executes the strategies.

This ambiguity is perceived as a business advantage by several interviewees. For example, one interviewee said (2): "We work under a very nice model whereby nothing we manage belongs to us, it all belongs to the client. You have to be very clear about that. That is to say; all that information belongs to [name of the party]. The person responsible for storing it is me, but the party is responsible for the use of that data".

The problem is that this model makes it difficult to know who should be held responsible when abuses are committed. This ambiguity was evident in a case in which the students of a university reported that the university's databases were being used to send messages promoting the rector's wife's political campaign. The rector denied the accusation, explaining that he had hired a communications agency, but that "they do not ask my permission to send messages and carry out the campaign" [31].

When the agency was consulted by another media outlet, they assured them that the official university databases were not used, and that data was collected using an unofficial Facebook page for faculty students [32]; this does not explain why text messages were sent to students' cell phones, since telephone numbers are not usually made public on this social network.

It is encouraging that citizens are starting to gain awareness about the importance of whether candidates are making appropriate use of their personal data, and that public pressure is beginning to be placed on preventing misuse. However, the problem is that the way in which the structure is designed makes it difficult to know who should be held responsible and how the information under question was obtained.

### **3. Politicians access some personal data on citizens through the *dark social*.**

Instant messaging services have become one of the main communication tools for Colombians. In consequence, their use in political communication and in electoral campaigns has shot up since the 2016 referendum on the endorsement of the peace agreement, in which WhatsApp became a vehicle for the transmission of messages with political objectives. This was the first campaign in which it became evident that “negative campaigning had shifted over to social platforms and in many cases misinformation was massively widespread, significantly affecting democratic transparency” [33, p. 66]; a process that was carried out largely through this messaging service.

It is for this reason that traces of the use of these tools in political campaigns were sought in the course of this investigation. It is important to note that WhatsApp, like all messaging applications, is part of what is called *dark social*. This expression has two different but related meanings. In network theory, this refers to “a community that is perceived as having great secrecy and influence hidden within” [34, p. 1]. Whereas, in the media, this term refers to traffic that, although it comes from social sources, does not have a clear origin, and therefore “is essentially invisible to most analytics programs” [35].

These two meanings point to the two key elements of this phenomenon. On the one hand, tracing the origin of the messages is practically impossible, since the platform erases all traces that can give information, such as its metadata or its history. On the other hand, the social structures and hierarchies that shape the propagation mechanisms of these messages are also closed and therefore difficult for anyone who does not belong to them to decipher. Although these features have made it possible for these applications to become important tools in internet user privacy protection, they become obstacles when it comes to investigating the flow of messages and the structure of the social networks that are built through them. For these reasons, the findings of this part of our research are partial and limited. To validate them, a more extensive investigation would be necessary, with a more precise methodology that is more focused on this phenomenon.

Nevertheless, almost everyone interviewed claimed to have some knowledge of how communication strategies work on WhatsApp. For the purposes of this investigation, it was interesting to note that these techniques are also based on data collection and the misuse of personal data. When one of the interviewees (3) said he knew how these disinformation operations were planned through the *dark social*, he described them in these terms: “Someone comes along and says: ‘all right, I have 1,000 phone numbers, and I’ll send a message to them’. There are also people who are, let’s say, influencers on WhatsApp. Why? This is someone who, in fact, has never been a politician, but has 1,500 stored numbers in their cell phone”. This testimony was only one among several obtained in interviews, which describe a similar method: a person with many contacts on their cell phone “lends” them to a politician to spread a message.

Again, there are different potential interpretations of whether or not this is an abuse. Anyone’s lists of phone numbers are considered databases for personal use by the law, and for that reason they are not subject to data protection requirements. However, when these lists and chains are used for commercial purposes, it seems obvious that authorization ought to be requested<sup>5</sup>. So it’s worth wondering whether this use for political purposes has a commercial intention or not. According to several interviewees, there are occasions in which the person who “owns” the contacts receives money for sharing them with the politician, and in those cases the commercial intention is certainly clear. Nevertheless, it’s not hard to imagine other cases in which a person simply wants to exercise their right to talk about politics with their friends, or to campaign for a candidate without coercing anyone. In this case, the line is rather fuzzy. It is legitimate for a person to exercise political autonomy through social networks and their personal contact networks, but when this is done in a systematic organized way, perhaps the regulation ought to be stricter to prevent abuses.

The problem is two-fold: from the outside it is difficult to distinguish one thing from the other and the law, once again, fails to offer clarifications to better understand this specific case.

#### **4. Conclusions**

The collection, storage and processing of personal data are the condition of possibility for a wide variety of techniques and tools of digital communication with political and electoral ends. On the one hand, the enormous amount of data that Facebook keeps on its users is used by politicians

---

<sup>5</sup> Thanks to Germán Realpe for clarifying this point.

with highly diverse electoral strategy objectives. They access the data through brokers whose techniques are essentially similar to those used in commercial advertising.

On the other hand, a significant proportion of candidates and parties use their web presence to collect citizens' data, but do not usually take sufficient measures to protect the personal information of their voters. They do not take basic computer security measures, nor do they offer sufficient information about their data protection policies, nor do they use practices to protect the best interests of citizens and safeguard their democratic guarantees. In addition, Colombian data protection regulation has failed to protect citizens from having their contact information used against their will for political canvassing purposes (notwithstanding the fact that they may have given their consent) even though digital strategists recognize that complying with this regulation is part of the rules of their work and that they are at risk when data is used inappropriately. Finally, there is some evidence of the use of personal data in *dark social* tools, particularly in WhatsApp, although more detailed information is needed for this to be confirmed.

This investigation has shown that awareness of data protection rules does not mean that parties, candidates and agencies are clear about how they can use people's data in their campaigns. This is because there is no express legal framework on the use of data in political information, which is something that people are beginning to see as a sensitive topic as it may jeopardize their privacy and serve to manipulate and misinform. Among other things, the subcontracting model with which these digital strategies are carried out dilutes responsibility when abuses take place. The ambiguity thus generated allows data usage that is not necessarily in line with the interests of citizens, and the great frequency with which this occurs could indicate structural weaknesses in data protection regulation that ought to be corrected.

However, the fact that those responsible for the digital communication of parties and candidates begin to recognize the misuse of data as a risk to their business could indicate that a critical attitude is emerging about this type of practice and its possible implications. Although it has become commonplace to say that "data is the new oil", the raw material of a myriad of corporate tools and a source of wealth that must be exploited, the cautious attitude revealed in this study could be sign of a change in perspective on personal data processing, and that in the future some actors may choose to do so only when absolutely necessary and worth the risk<sup>6</sup>.

This study is only a preliminary inquiry into the use of personal data in political campaigns. Its tentative conclusions could be extended and qualified with more ambitious methodologies, such

---

<sup>6</sup> Many thanks to Juan Diego Castañeda for this conclusion.

as ethnography or participant observation. The conclusions drawn, therefore, are not meant to be definitive, but rather to encourage more research on the subject.

Moreover, it ought to be borne in mind that this study was carried out before Cambridge Analytica's poor handling of personal data came to light and Facebook took action in response to the public relations crisis that arose after these revelations. Indeed, it is possible that the announcement that the social network will stop sharing information with some "large data brokers" [36] and stop allowing advertisers to segment their advertisements with data collected by certain third parties may affect the future viability of some of the practices described in this study, but at this point it is impossible to predict this with certainty.

## **Annex 1: List of parties and agencies**

### **Bibliography**

- [1] DANE, "Reloj de población," 2018. [Online]. Available: <http://www.dane.gov.co/reloj/>. [Accessed: 06-Apr-2018].
- [2] Banco Mundial, "Población rural (% de la población total)," 2016. [Online]. Available: <https://datos.bancomundial.org/indicador/SP.RUR.TOTL.ZS?view=chart>. [Accessed: 06-Apr-2018].
- [3] DANE, "Pirámide de población total según sexo y grupos quinquenales de edad," 2015. [Online]. Available: <https://geoportal.dane.gov.co/midaneapp/pob.html>. [Accessed: 06-Apr-2018].
- [4] Registraduría Nacional del Estado Civil, "Partidos y movimientos políticos," 2018. [Online]. Available: <https://wsr.registraduria.gov.co/-Partidos-y-movimientos-politicos,317-.html>. [Accessed: 06-Apr-2018].
- [5] Registraduría Nacional del Estado Civil, "69 grupos significativos de ciudadanos se han inscrito para elecciones de 2018," Bogota, 2018.
- [6] J. L. Peñarredonda, "Colombia llegó a 5 millones de conexiones de banda ancha," *Enter.co*, 17-May-2012.
- [7] Ministerio de las TIC, "Boletín trimestral de las TIC. Cifras tercer trimestre de 2017," Bogotá, 2017.
- [8] Ministerio de las TIC, "En el 2017 las transacciones digitales en Colombia aumentaron 24% con respecto al 2016," 2018. [Online]. Available: <http://www.mintic.gov.co/portal/604/w3-article-71542.html>. [Accessed: 06-Apr-2018].
- [9] IAB Colombia, "Reporte de inversión en publicidad digital," Bogotá, 2017.
- [10] Portafolio, "Facebook tiene 17 millones de usuarios diarios en el país," *Portafolio*, Bogota, 09-May-2017.
- [11] El Tiempo, "Twitter aumenta en 15% el número de usuarios en Latinoamérica en 2016," *El Tiempo*, Bogotá, 02-Dec-2016.
- [12] A. M. Luzardo, "¿Cuáles son las aplicaciones preferidas por los colombianos?," *Enter.co*,

31-Jul-2017.

- [13] A. Gomez-Suarez, "Peace Process Pedagogy: lessons from the no-vote victory in the Colombian peace referendum," *Comp. Educ.*, vol. 53, no. 3, pp. 462–482, Jul. 2017.
- [14] J. Ramírez Prado, "El No ha sido la campaña más barata y más efectiva de la historia," *Asuntos Legales*, Bogotá, 04-Oct-2016.
- [15] D. Coronell, "La grabación," *Semana*, Jun-2017.
- [16] E. M. Restrepo, "Online Deliberation in the Wake of the Colombian Peace Process," Coral Gables, Jun. 2017.
- [17] P. Medina Uribe, "In Colombia, a WhatsApp Campaign against Posverdad," *The Wilson Quarterly*, Washington D.C., 2018.
- [18] *Semana*, "¿Alguien espía a los negociadores de La Habana?," *Semana*, Bogotá, Mar-2014.
- [19] *El Tiempo*, "Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue," *El Tiempo*, Bogotá, 23-Jan-2015.
- [20] J. L. Peñarredonda, "Buggly, la comunidad en la que el Ejército camufló a sus hackers," *Enter.co*, Bogotá, 05-Feb-2014.
- [21] G. Realpe and J. L. Peñarredonda, "Me arrepiento de haberme involucrado en política': hacker Sepúlveda," *Enter.co*, 10-Apr-2016.
- [22] J. L. Peñarredonda, "Detrás de Buggly: la historia de la fachada Andrómeda," *Enter.co*, Bogotá, 09-Dec-2015.
- [23] Fiscalía General de la Nación, "Condenado hacker Andrés Sepúlveda por interceptar a negociadores de paz en La Habana," 2015. [Online]. Available: <https://www.fiscalia.gov.co/colombia/noticias/condenado-hacker-andres-sepulveda-por-interceptar-a-negociadores-de-paz-en-la-habana/>. [Accessed: 07-Apr-2018].
- [24] B. Bimber, "Digital Media in the Obama Campaigns of 2008 and 2012: Adaptation to the Personalized Political Communication Environment," *J. Inf. Technol. Polit.*, vol. 11, no. 2, pp. 130–150, Apr. 2014.
- [25] Ministerio de las TIC, "Colombia es uno de los países con más usuarios en redes sociales en la región," 2014. [Online]. Available: <http://web.archive.org/web/20141003231844/https://www.mintic.gov.co/portal/604/w3-article-2713.html>. [Accessed: 06-Apr-2018].
- [26] Fundación Karisma, "Derechos de la Mujer en Línea. Informe de país: Colombia," Bogotá, 2015.
- [27] J. van Dijk and K. Hacker, "The digital divide as a complex and dynamic phenomenon," *Inf. Soc.*, vol. 19, no. 4, pp. 315–326, 2003.
- [28] Ministerio de las TIC, "Encuesta de acceso, uso y apropiación por parte de las mujeres de las TIC en Colombia," 2018.
- [29] Superintendencia de Industria y Comercio, "Resolución 13790 de 2016". Bogotá, 2016.
- [30] C. Botero, "Personalizar Tullave es entregar un cheque en blanco," *La Silla Vacía*, 2017. [Online]. Available: <http://lasillavacia.com/silla-llena/red-de-la-innovacion/historia/personalizar-tullave-es-entregar-un-cheque-en-blanco-parte>. [Accessed: 02-Apr-2018].
- [31] C. Hernández Osorio, "Los mensajes en la Sergio Arboleda que invitan a votar por la

- esposa del Rector,” *La Silla Vacía*, 06-Mar-2018.
- [32] Seguimiento.co, “El audio que vuelve a enredar a la Sergio Arboleda con campaña de la esposa del rector,” *Seguimiento.co*, 08-Mar-2018.
- [33] J. J. Verjel Torrado, “Plebiscito por la paz en Colombia, una disputa más allá del contenido de los acuerdos,” *Marco Rev. Mark. y Comun. Política*, vol. 3, pp. 57–76, 2017.
- [34] S. Karthika and S. Bose, “IBeH: Naïve Community Detection Methodology for Dark Social Network,” in *Proceedings of the International Conference on Informatics and Analytics - ICIA-16*, 2016, pp. 1–4.
- [35] A. Madrigal, “Dark Social: We Have the Whole History of the Web Wrong,” *The Atlantic*, New York, Oct-2012.
- [36] D. Ingram and J. Fioretti, “Facebook cuts ties to data brokers in blow to targeted ads,” *Reuters*, 28-Mar-2018.