The dark side of digital politics: understanding the algorithmic manufacturing of consent and the hindering of online dissidence

Emiliano Treré

Emiliano Treré is Associate Professor at the Autonomous University of Querétaro (Mexico) and Research Fellow at Lakehead University (Canada). He has published extensively in top-ranked international journals and books on digital activism, media ecologies, media practices, and the benefits and challenges of social media for contemporary social movements. He is coeditor of ‘Social Media and Protest Identities’, (Information, Communication and Society, 2015) and ‘Latin American Struggles and Digital Media Resistance’, (International Journal of Communication, 2015).

Abstract

Various strands of literature on civic engagement, ‘big data’ and open government view digital technologies as the key to easier government accountability and citizens’ empowerment, and the solution to many of the problems of contemporary democracies. Drawing on a critical analysis of contemporary Mexican social and political phenomena, and on a two-year-long ethnography with the #YoSoy132 networked movement, this article demonstrates that digital tools have been successfully deployed by Mexican parties and governments in order to manufacture consent, sabotage dissidence, threaten activists, and gather personal data without citizens’ agreement. These new algorithmic strategies, it is contended, clearly show that there is nothing inherently democratic in digital communication technologies, and that citizens and activists have to struggle against increasingly sophisticated techniques of control and repression that exploit the very mechanisms that many consider to be emancipatory technologies.

Introduction: coming to terms with techno-optimism within digital democratic participation

There is a shared tendency in different strands of the literature on civic engagement, digital activism and protest movements – as well as in reflections on the possibilities afforded by open ‘big’ data for increasing democratic participation – to view digital technology as the key to easier government accountability, and the panacea that can easily solve the various issues that plague the worn apparatus of contemporary public institutions. For instance, in recent years the literature on social movements and digital media technologies has often reduced diverse complex socio-technical configurations and cultural contexts to simple,
easy-to-understand Twitter or Facebook ‘revolutions’. At the same time, the technological
developments enabling the publication of Open Data and the tools and capacities to engage
with it have been at the forefront of techno-optimism in the transparency and accountability
field. These developments hold the potential for making vast amounts of government data –
including budget and procurement information – widely available to huge numbers of
citizens, who, as the hypothesis goes, will then be able to easily analyse and use the data to
hold governments to account. However, various authors have started to unravel the
ambiguities, promises and perils of the open government phenomenon (Davies and Bawa
2012; Yu and Robinson 2012).

Meanwhile, the ‘big data’ phenomenon has gained remarkable momentum across a wide
range of industries and fields, as well as academia. Like many ‘buzzwords’ that have entered
the contemporary debate, ‘big data’ refers to a plethora of interconnected social, economical
and technological phenomena, with reflections about the benefits and challenges of
analysing “massive quantities of information produced by and about people, things and their
interactions” (Boyd and Crawford 2012:1) at their centre. The potential of large-scale data-gathering has been praised for its unprecedented revolutionary possibilities, which could
include a decisive improvement in the ways citizens and governments interact.

Diverse voices have begun to question uncritical views of these phenomena, for example
providing more nuanced reflections on the pitfalls and threats of ‘big data’ (Boyd and
Crawford 2012; Couldry and Powell 2014; Crawford, Gray and Miltnor 2014; Tufecki 2014).
These authors contend that ‘big data’ is not merely a technological issue, but first and
foremost a ‘mythology’ (Mosco 2014), an emerging worldview that has to be interrogated,
and critically engaged with, not incontrovertibly accepted and applauded. Thus,
understanding ‘big data’ means exploring the consequences of the computational turn
across multiple disciplines, and through the alterations it creates in the spheres of
epistemology, ontology and ethics. It also means examining the limitations, errors and
biases in the gathering and interpretation of these massive quantities of information, as well
as access to it. In sum, it means untangling the processes at the core of our ‘algorithmic
culture’ (Hallinan and Striphas 2015).

Other critical voices that tackle the limits, risks and threats of digital communication
technologies in relation to democratic processes have emerged (Fuchs 2014; Dean 2005).
Even so, most accounts of experiences and case studies related to the use and
appropriation of digital technology in relation to civic engagement still put much emphasis on
the use of online platforms to simply ‘fix’ feedback loops, allowing citizens to provide
feedback on public services, and the predominant mood remains optimistic about the potential opportunities that technology can offer for citizens to hold governments to account.

One of the key lessons of the Making All Voices Count programme is precisely that the issue of accountability should be framed as a complex political problem, rather than as a technical one. But, as has been shown in recent studies (Morozov 2013; Treré and Barranquero 2013), accountability has often been seen as a matter of simply ‘finding the right technological problem-solving tool’. Furthermore, the controversial question of obtaining government responsiveness has been usually treated in technology studies as a linear and straightforward procedure (McGee 2014), rather than as a process that entails dealing strategically with power relations that influence which voices will be heard, thus constituting a delicate dance between mechanisms that promote citizens’ voice and efforts to change government behaviours. However, the voice of citizens does not speak in a vacuum, but rather within the boundaries and the limitations of contemporary neoliberalism, that systematically denies and undermines it (Couldry 2010).

Much of the current focus neglects the ways in which governments can and do use digital technology to survey and undermine citizens’ attempts to hold them accountable. Instead, something that the recent National Security Agency–Snowden scandal made clear is that these technologies are used more to spy on us and limit our freedom, than to provide us with useful tools to improve the functioning of democratic institutions.

This article will try to counteract the techno-optimistic bias by providing and examining some examples that clearly illustrate the various complications emerging from the deployment of digital technologies by governments and parties, and appropriations by citizens and activists. The article will draw on a critical analysis of various contemporary Mexican social and political phenomena, and on a two-year-long multimodal ethnography that relies on the triangulation of different methodologies: fifty individual interviews with activists of #YoSoy132; four group interviews with protesters from Mexico City, Guadalajara and Querétaro; several short periods of participant observation during 2012 and 2013; and a qualitative content analysis of digital media and online platforms. Based on the exploration of the Mexican resistance scenario, this article will clearly show that digital platforms can be used by government and parties in order to create consent online, control and monitor citizens’ activities, and undermine dissent on social media platforms. It also shows that the appropriation of digital communication technologies by activists, far from being a linear and unproblematic practice, is instead afflicted by everyday frictions, conflicts and struggles.
The article begins by describing the context of the 2012 Mexican elections and the *activism* phenomenon. It goes on to explore the algorithmic manufacturing of consent and undermining of dissent, focusing on the emergence of the #YoSoy132 movement and the perils of its digital media practices, in particular the so-called ‘Cossio case’. Finally, it outlines some broader considerations for the study of digital politics and sketches future scenarios.

**The 2012 Mexican elections**

During the run-up to the 2012 Mexican general elections, the Institutional Revolutionary Party (PRI) – which governed for 70 years, prior to the election of the National Action Party (PAN) in 2000 – led in several polls. The PRI candidate was a young and attractive man, whose image dominated the media: Enrique Peña Nieto (EPN). As documented by various investigative journalists (Tuckman 2012; Villamil 2010), for six years the Mexican media titan Televisa had crafted EPN's candidacy, at the same time as delegitimising his left-wing opponent Manuel López Obrador. The Mexican *telecracy* – the media television duopoly Televisa-TvAzteca, which controls 99% of the market (Huerta-Wong and Gómez 2013) – has been described as a ‘wild power’ (Trejo 2004), capable of a powerful impact on political decisions. Before 2012, Mexican politicians had never considered politics through digital technologies a priority, relying instead on the powerful media propaganda apparatus provided by television as their main channel for campaigning (SánchezEspino 2012).

**The *activism* phenomenon**

The 2012 elections witnessed what some saw as an explosion of digital politics, with politicians embracing social media to spread their messages and to engage in dialogue with citizens. But they mostly considered online spaces as sites for both the premeditated construction of consensus and the artificial, algorithmic construction of consent, rather than environments for reinforcing democracy through dialogue, participation and transparency.

Octavio Islas has framed this behaviour as “authoritarian engineering” (Islas 2015:1), the adoption by Mexican politicians of dirty online strategies which reveal their incapacity and refusal to develop political campaigns that can build a trustworthy base of sympathisers and followers in cyberspace, and the very opposite of citizen participation. A video posted on YouTube the day before the second presidential debate, *The Truth of Peña Nieto on Twitter*, revealed the existence of organised groups of so-called PRI *activistas* (*activists*), dedicated to tweeting according to the instructions of EPN’s campaign leaders, and trying to counteract, isolate or sabotage criticisms of PRI from civil society actors or other citizens.
The film shows a campaign operator telling activists how to overturn hashtags negative to the campaign.

The activist phenomenon is controversial. The network was formed in December 2009, and activist leaders have always claimed to be nothing more than a network of independent young volunteers and PRI supporters\(^{\text{iv}}\). But, as the online video shows, and as other researchers have demonstrated (Figueiras 2012), the organisation of an estimated 100,000 activists (Islas 2015) was used systematically during the PRI campaign to successfully spread and situate Peña Nieto’s image on digital media platforms. In particular, the network was ‘activated’ during periods when Peña Nieto’s public image suffered, for instance after his speech at the Guadalajara International Book Fair, when he was unable to accurately name three books that had influenced his life, and when the #YoSoy132 movement emerged. In order to counteract embarrassments and negative public image, Peña Nieto’s media team intensified the directed online activities of the activists. Although one of Peña Nieto’s campaign managers (who later became Secretary of Education) acknowledged\(^{\text{v}}\) in May 2012 that 20,000 activists were tweeting without receiving any monetary compensation, many thousands of others were hired, revealing the possibilities for impacting, distorting and manufacturing public opinion within digital environments that institutional parties with immense financial resources like the PRI have at their disposal.

**The algorithmic manufacturing of consent**

The use of digital strategies in Mexican electoral politics dates to the 2011 elections for the Governor of the State of Mexico, but the 2012 general election saw them refined and broadened. Studies of the social media strategies of Mexican politicians during the 2012 campaign find that intensified use of digital technologies did not correspond to an increase in democratic participation or dialogue between candidates and voters, but was instead constituted by a massive deployment of strategies including: the creation of false universes of followers; the use of software robots (bots)\(^{\text{v}}\) to automatically generate tweets; and the hiring of trolls (people who tweet in favour of a candidate, and against their opponent); and ghost followers (empty accounts that boost a candidate’s followers). By employing these strategies, candidates discarded the possibility of using digital technologies to include voters’ feedback into their decisions, or incorporate democratic visions into their ways of doing politics (Ricaurte Quijano 2013). An article on the phenomenon in the MIT Technology Review (Orcutt 2012) discusses dangers of “large-scale political spamming”, and the need to develop countermeasures to prevent the expansion of this phenomenon to other political scenarios.
The algorithmic undermining of dissent

The algorithmic construction of consent goes hand-in-hand with the undermining of critical voices. As carefully documented by several bloggers\textsuperscript{v}, EPN critics mobilising for the #MarchaAntiEPN (March against Peña Nieto) on Twitter were systematically attacked and blocked online. As Verkamp and Gupta (2013) demonstrate, dissident voices were ‘drowned’ on various occasions by orchestrated bot attacks. Since 2012, political activists and civil society organisations have denounced the dangers of these attacks, arguing that they criminalise protest and segregate dissident voices\textsuperscript{vi}, pointing out the need to act immediately to prevent more serious future threats. Unfortunately, political strategies that rely on digital technologies to artificially boost consensus have been enhanced in the years since the election, up to the point where they have become an essential component of the government’s modus operandi, used repeatedly during 2013.\textsuperscript{vii}

One case is particularly illuminating, described by philosopher Carlos Soto Morfín as a clear example of techno-authoritarianism\textsuperscript{viii}. A study, commissioned by the news programme of a liberal Mexican journalist and carried out by social network and data-mining agency Mesura, exposed the massive use of bots to build an illusion of online support for a controversial energy reform (Aristegui Noticias 2015). Mesura documented the systematic deployment of bots to tweet and re-tweet in support of the reform, discovering that the time gap between the sending of a supportive original message and its re-tweeting was too short to be accomplished by a human being. Morfín, one of the authors of the study, concludes by warning about the risks to which citizens are exposed in an era when the importance of digital politics is growing day by day, and when those in power have no ethical problems with manipulating public perception.

On 26 September 2014, a group of students departed the Ayotzinapa Rural Teachers’ College for a protest in the city of Iguala, about 130km away. They never arrived. Exactly what happened remains unknown, but we do know that at least three students were killed and another 43 remain missing. The Mexican government’s official version is that the students were killed after being handed over to the Guerreros Unidos cartel on the orders of the mayor of Iguala, but investigations conducted by the Mexican critical magazine Proceso and the US publication The Intercept portrayed a darker picture of government complacency. After the event, several activists and citizens started to protest on social media, and the Twitter hashtag #YaMeCanse (I am tired) – which expressed the feeling of not being able to take any more violence or permanent insecurity – soon became the core for mobilising and spreading information. But journalist Erin Gallagher, who covers protests for the online magazine Revolution News\textsuperscript{ix} soon noticed something atypical in the search results for the
YaMeCanse hashtags: that they were flooded with tweets including the hashtag but no other content apart from random punctuation marks. The accounts that were tweeting this kind of empty content were bots: they lacked followers, and were tweeting automatically. The noise they created made it difficult for citizens to share information using YaMeCanse, and the hashtag consequently dropped out of Twitter's trending topics. Mexican blogger and data-mining analyst Alberto Escorcia has discovered a reliable way of detecting bot accounts by examining the number of connections a Twitter account has with other users, and has been documenting the use of bots in Mexico to sabotage protests by preventing information from spreading, and to send death threats to specific activists. For example, since February 2015, anthropologist, activist and blogger Rossana Reguillo has received regular death threats on various social media platforms. Particularly harsh attacks via Twitter lasted more than two months, and data-mining analysis of the Twitter campaign showed that bots and trolls were responsible for the majority of the attacks.

Another social media is possible? The YoSoy132 movement

In the run-up to the 2012 elections, EPN's path to the presidency seemed unstoppable. But on 11 May, something unsettled his image as the only available option for Mexico. He arrived at the private, religious IberoAmerican University in Mexico City to give a lecture, an event that PRI expected to run in an uncomplicated way. However, during the candidate's presentation, several students began to question him about police repression and the killings that occurred when he was Governor of the State of Mexico. When EPN justified those violent repressions, tensions rose, and he had to leave the university surrounded by a security cordon. Immediately after the event, PRI politicians described the students as violent, intolerant fascist thugs, going so far as to deny that they were students. At the same time, the Mexican telecracy and the newspaper chain Organización Editorial Mexicana presented versions of the event which portrayed EPN as a hero who had survived a boycott organized by the Left. This biased coverage led 131 IberoAmerican students to publish a video on YouTube in which they displayed their student credentials and read their out their names to the camera. This powerful act of reclaimed identity marked the start of the YoSoy132 movement, when the phrase ‘131 students from Ibero' quickly became one of the trending topics on Twitter in Mexico, and other students began to join the protest, stating ‘I am 132'. This led to the creation of the hashtag which went on to identify the whole movement. While the dirty digital strategies of institutional politics were dominating cyberspace, these students proved to the world that digital technologies could be used also to spread critical voices, mobilise support, organise protests and foster collective identification processes.
The digital perils of a networked movement

The celebratory literature that has developed around the #YoSoy132 movement proclaims the role of social media in the development of a ‘fifth state’ and in the birth of a ‘Mexican spring’ (Islas and Arribas 2012), and frames digital technologies as a powerful media alternative to the Mexican telecracy (Andión Gamboa 2013). My research depicts a different scenario, where everyday frictions and struggles, issues of exploitation, dataveillance and control – together with constant attempts at delegitimisation – continuously plague protestors’ use of digital technologies. Activists’ social media communications are constantly afflicted by clashes, struggles and discord. These divergences come to manifest themselves in terms of daily interactions as concern and discomfort with integrating social media into protest practices. Issues of ephemerality and weak ties seep through movement interactions by raising questions of authority and belonging, played out in terms of conflicts over who has access to digital media, and what can be posted on social media platforms in the name of any given protest. These are illustrated by the Cossío case, in which a web platform was used to infiltrate the movement, gather data on activists and post two videos to try to undermine the reputation of #YoSoy132.

The Cossío case: web surveillance and video aggressions

In May 2012, a man named Manuel Cossío offered #YoSoy132 activists his digital expertise and a fully functional web portal, YoSoy132.mx. Only ten days after the emergence of #YoSoy132, Cossío entered the movement through one of its most prominent student activists, Saúl Alvídrez. While Alvídrez and other activists had already acquired the YoSoy132.com and the YoSoy132.com.mx domains, it was the YoSoy132.mx registered by Cossío that was finally adopted, thanks to Cossío’s rhetorical skills in selling the movement his “valuable, ready-to-go product” during various assemblies and meetings. Announced as the official page of the movement by various activists on their Twitter feeds and Facebook pages, this professional-looking website, fully integrated with possibilities for access and interactions with other platforms like Google and Facebook, was extensively adopted for debate, organisation, content spreading, and especially for the archiving of contributors’ data. But, after a month of intense use of the website, something strange occurred. On 18 June, two YouTube videos appeared on the home page of the #YoSoy132 portal and in the YouTube account ‘Yo Soy’.

In the first video, we see in the background the fixed image of the face of Saúl Alvídrez, at the same time as we hear his voice and see yellow subtitles that report his words. The audio, clearly recorded without his consent, appears as a combination of various of Alvídrez’ informal talks, in which #YoSoy132 student speaks about the movement and relations with
Andrés Manuel Lopez Obrador (the leader of the Left), and other leftist figures, especially a collective of directors, investigative journalists and other critical intellectuals named México, ahora o nunca (Mexico, now or never).

The second video is entitled *La verdad nos hará libres* (Truth will set us free) – a biblical quote, the motto of the IberoAmerican University, which was adopted as one of the principal slogans of the movement. Manuel Cossío speaks to the camera, reading a text where he expresses his profound disappointment on discovering that many leaders of the #YoSoy132 movement had been co-opted by left-wing politicians affiliated with the Party of the Democratic Revolution—party, such as Marcelo Ebrard, López Obrador and Alejandro Encinas.

Both of these online attempts at delegitimisation were the creation of Manuel Cossío Ramos, owner and manager of the YoSoy132.mx website. According to an inquiry carried out by the online investigative journalism website Contralínea in June 2013, Cossío was an agent of the Mexican Secret Service, the Centre of National Watch and Security, whose mission was to infiltrate the movement, steal data through the use of the Web platform, and destabilise the power balances within #YoSoy132 before the elections. Activists of the movement, flooded with activities, internal struggles and frictions, and having to deal with organisational challenges in the immediate days after the eruption of #YoSoy132, trusted Cossío and fell into the government’s ‘digital trap’.

The two videos caused controversy and conflict: Alvídrez had to leave the movement and the Mexican telecracy took advantage of the event to insinuate that the videos represented a clear proof that the Mexican movement had been manipulated from the beginning by the intellectuals of the Left. #YoSoy132 activists eventually realized that the platform was intended as a way to monitor, control and profile them and decided to migrate to another platform, yosoy132media.mx. This migration and the dangers related to the use of the other so-called ‘apocryphal web pages’ were officially announced on Facebook and spread through multiple Twitter accounts in order to inform citizens about the real intentions of Cossío and the nature of the fake portal; other users and supporters from the Mexican blogosphere also retweeted the information.

According to the Contralínea website, the platform was able to steal the information of more than seventy thousand citizens with yet unexplored consequences for the Mexican resistance. But we still do not have clear figures and data on the scope and the results of this operation of sabotage and surveillance by the Mexican government, and we almost
surely never will. The mechanisms of this kind of digital warfare remain opaque, secret and very difficult to decode. What this example clearly shows is the extent to which political control can use the technological platform through which opposition is carried out, stealing data and monitoring protest activities, controlling the information flowing through the platform, and exploiting it to compromise and destabilise the reputation of the movement. The same digital communication technologies that allow engaged citizens to organise, spread alternative information, and make the government accountable have been easily infiltrated and used against them.

Conclusions: the limits and future horizons of data activism

In contrast to celebratory accounts that in various disciplines and fields have conceived the increasing use of digital technologies as a way to make governments accountable, and solve most of the issues that plague contemporary political systems, this article, based on an exploration of social and political experiences of the Mexican context, has demonstrated that digital tools have been successfully deployed by parties and governments to manufacture consent, sabotage dissidence, threaten activists, and gather information without citizens’ consent.

Nowadays, institutions and parties cannot only count on the traditional channels of propaganda, such as the powerful and biased mainstream media apparatus, but can also use their vast financial resources in order to hire crowds of sympathisers that can boost their image on digital platforms, deploy armies of bots and trolls that can be activated to sabotage dissent and hinder critical voices on social media, and infiltrate movements with imposter techies who can use websites to steal sensible activists’ data.

Against these powerful strategies, activists have few digital weapons at their disposal, above all because they cannot count on huge economic resources. However, as we have seen throughout the article, some of them have started to use their technological skills in social network analysis and data-mining techniques in order to unmask and denounce these dirty strategies on various radical media outlets. Perhaps we can conceive of these tactics as ‘counterprotocol practices’ (Galloway and Thacker 2007) that use the same advanced technological tools that the powerful deploy to control us in order to make their strategies visible and accountable. This form of ‘data activism’ (Milan 2015) can empower citizens and activists in their quest for truth and accountability, but given the unbalanced distribution of power, these attempts remain feeble and seldom influence public opinion at the international level, or the effective counteraction of such dirty schemes.
Before singing the praises of digital communication technologies to make democratic institutions more accountable and reliable, we should recognise, understand and try to overcome the plethora of dangers and risks that are associated with them in the arena of digital politics. The algorithmic construction of consent and the artificial sabotage of dissent demonstrate that there is nothing inherently democratic in digital technologies. In order to guarantee that a plurality of critical voices is represented and can be heard, citizens have to struggle against increasingly sophisticated techniques of control and repression that successfully exploit the very mechanisms that many consider to be emancipatory technologies.

**References**


Commented [A1]: This link doesn’t work. Rosie, Duncan – is this still in the public domain or is it internal?

The new one I provide is working.


---
i Making All Voices Count is supported by DFID, USAID, Sida and Omidyar Network
ii https://www.youtube.com/watch?v=mcy5uT4TygA
iii http://mexico.cnn.com/nacional/2012/05/18/quienes-son-los-estivistas-y-por-que-apoyan-a-pena-nieto
A ‘social bot’ refers to a ‘computer algorithm that automatically produces content and interacts with humans on social media, trying to emulate and possibly alter their behavior’ (Ferrara et al. 2014: 1-2). Some are benign, but many designed the purpose of harmfully manipulating social media discourse, for instance by artificially inflating the support of a candidate during the elections.


See the following websites for a detailed list of cases where bots were systematically deployed in the Mexican context in the last few years: http://www.sinembargo.mx/opinion/07-01-2014/20465; http://loquesigue.tv/

The expression techno-authoritarianism has been adopted in other contexts to refer broadly to uses of digital technologies that reinforce hierarchies, and leadership while pretending to enhance participatory democracy (Treré and Barassi 2015).

Research interview with Laura, 11 April 2013.

These findings were anticipated by articles on the critical blog SinEmbargo and by the magazine Proceso, and further analysed on the Revolución 3.0 blog.