Digital disintermediation, technical and national sovereignty. The Internet shutdown of Catalonia's "independence referendum"

To cite this article: Sampedro V, López-Ferrández FJ, Hidalgo P. Digital disintermediation, technical and national sovereignty: The Internet shutdown of Catalonia's 'independence referendum.' *European Journal of Communication*. May 2021. doi:10.1177/02673231211012143

Abstract

This article analyses the digital shutdown experienced in Catalonia within the framework of the independence referendum of 1 October 2017, which had been declared illegal by Spain's Constitutional Court. We question the notion of digital disintermediation and examine how Internet control and blackout processes are not exclusive to authoritarian political systems, but have instead begun to develop in Western democracies in situations of socio-political crisis. We analyse the type of shutdown implemented in Catalonia, the players (both institutional and corporate) taking part in the process, and the resistance strategies implemented by civil society to maintain the flow of digital communications. In our conclusions, we reflect upon the implications of the events that took place in Catalonia for the future of digital sovereignty and suggest further lines of research for monitoring similar shutdown processes.

Keywords

Digital sovereignty, Internet shutdown, Disintermediation, Catalonia, Independence

1. Introduction

We present the first academic analyses on the Internet control and to impede Catalonia's independence referendum of October 1st 2017 (known as "1-O") aiming to contribute to the increasing research on digital shutdowns in general. The object of study is neither this referendum nor the Catalan independence "process", and even less the dispute over their legitimacy. What we are interested in here is to reflect upon present and future Internet-related civil liberties. This specific Internet shutdown –like all others– preceded and complemented curtailing of political rights.

We shall be using the terms "shutdown", "blackout" and "kill switch" without distinction to discuss two types of measures: those that entail the "withdrawal" of

certain websites and others that involve a partial or generalised blockage of access to the Internet for specific geographic areas, access points or users. The events of 1-O provide a paradigmatic case study: a political process promoted by the regional government and the majority of Catalonia's local authorities, thus all subject to both Spanish and European Union (EU) law. On October 1st 2017 took place the first Internet shutdown in the EU –which did not recognise the legitimacy of either the referendum or its results (Perales-García and Pont-Sorribes, 2018)–. The measures adopted could well be applied to future digital mobilisations.

We examine whether there were any violations of the rights to free speech and political participation. We also analyse the resistance offered by Catalonia's government and civil society to maintain their digital communications.

2. The myth of disintermediation, the shutdown of the digital public sphere and technological sovereignty

Much academic literature has highlighted the democratising potential of digital ICTs, fostering self-communication, self-organisation, collaborative processes and networked collective action (Rheingold, 2002; Castells, 2009; Shirky, 2010). A sort of "digital mythology" trumpeted communicative disintermediation, but the notion has been called into doubt by the processes of corporate concentration and privatisation. State and corporate surveillance affect internet users' practices, threatening Internet neutrality and fostering user polarisation, segmentation, fake news and digital marketing (Benkler et al., 2017; Marwick and Lewis, 2017).

Rather than digital disintermediation, Couldry and Hepp (2016) point out that we experience "deep mediatisation". A large amount of our political, economic and social structures depend upon digital media and technologies. Besides, the infrastructures and devices to which we are hyperconnected, far from being based on open logics, are operated by private undertakings (Splichal, 2019). On the other hand, countless initiatives develop an autonomous digital environment based on free open-source software, underpinning a productive framework and model inspired by the principles of the social and solidarity-based economy (Haché, 2017). Indeed, "digital sovereignty" (Haché, 2014; Beltrán, 2016) requires that technologies be managed with infrastructures and practices that guarantee collective privacy, knowledge and benefits. Nevertheless, the "algorithmic culture" (Striphas, 2015) and "datafication" (Van Dijck, 2014) impose political and commercial logics, calling into question the Internet's "independence" and "sovereignty", in the presence of the public powers' passivity, acquiescence or inability to exert control (Fenton, 2016).

An Internet shutdown has cultural and symbolic implications, with the dominance of political and corporate propaganda. On a structural level, it extends the systematised monitoring and profiling of users. Internet shutdowns are the clearest example of the

infringement of the digital freedoms of information and expression, and constitute a growing phenomenon worldwide.

Although we take a political economy approach, there is a growing body of legal literature concerning our case study. Since the late 90's the European Court of Human Rights has developed some "guiding principles" concerning online freedom of expression and information in relation to copyright infringement, hate speech or apology of terrorism (Akdeniz, 2013, Voorhoof, 2020). Internet platforms play an increasing relevant role in the so called "privatization of censorship" by exerting a "censorship de facto" and a "delegated censorship" (Monti, 2019). Previous studies of European Internet control mechanisms pointed that "they can only work properly with the political or financial support of the state and the market sphere" (Parti and Marin, 2013: 156). In Spain Teruel (2014: 70-71) has argued that "transparency and plurality were required in case filters were imposed by servers or search engines [… given ...] the business landing on the Net and the tendency to concentration can endanger pluralism. As a general trend, Louis Cook (2006: 373) concluded that "in the EU arena, the desire to control and regulate the internet is taking precedence over measures to promote freedom of expression and freedom of enquiry online".

3. Internet shutdowns: typology and trends

Freedom House (2017) defines Internet shutdowns as "intentional restrictions on connectivity for fixed-line internet networks, mobile data networks, or both". Access Now, another organisation defending digital rights, adds the responsibility of the political establishment, indicating that an Internet shutdown occurs when someone, normally a government, intentionally interrupts the Internet or mobile applications to control what people say or do[1]. These actions can only take place with the collaboration, voluntary or coerced, between governments, telecom companies and Internet service providers. The above civic organisations agree that their use is spreading and denotes a lack of democratic quality. Academic literature qualifies Internet shutdowns as illiberal and authoritarian practices (Michaelsen and Glasius, 2018; Hintz and Milan, 2018), regarding them as a matter of human rights.

Table 1 suggests a typology of Internet shutdowns based on the following parameters: political system in which implemented, recognition strategy, activation mechanisms and scope. These parameters differentiate the distinctive control mechanisms compiled in reports taking a comparative perspective (Acess Now, 2018, 2019).

The legal/political context is a distinguishing feature of Internet shutdowns, as fundamental rights are afforded different levels of protection in: democratic

[1] Deji Bryce Olukotun, Senior Global Advocacy Manager at Access Now. *DW Akademie*: https://www.dw.com/en/internet-shutdowns-an-explainer/a-36731481

environments (where safeguards are high or very high), authoritarian or dictatorial environments (where there is little or very little protection) or failed states, which offer no protection whatsoever.

There are different ways in which political powers restrict the Internet and justify their interventions. First-generation practices are selective repression actions focused on specific objectives. The blockade of certain web pages or the disconnection of specific users or geographical areas from concrete (or general) internet services, are examples of first generation practices. Hand-in-hand with these go the viralisation of an official account, which can encounter oppositional or dissident narratives. Second-generation practices lack a specific goal instead. Political powers do not seek to bolster a democratic reputation before national or international public opinion, and do not always create coordinated or coherent justifications. Elites take for granted and take advantage of "splinternet", a term first coined by Clyde Wayne Crews (2001) to refer to "owned Internets-proprietary "Splinternets" where prespecified ground rules regarding privacy and other governance issues replace regulation and central planning– may be superior." This libertarian and positive perspective conflicts with the "cyber-balkanization" or "internet balkanization" where national and commercial interests justify without further justification the control of public authorities over an increasingly splinted Internet (Malcomson, 2015).

There are two types of activation mechanisms: preventive and reactive shutdowns. In the former, the authorities anticipate a potential threat against public order or national security. Reactive blackouts, on the other hand, are implemented simultaneously with or subsequent to the detection of a threat.

Lastly, we break down shutdowns based on their scope, distinguishing between partial and total blackouts. The latter affects all communication structures: fixed and mobile telephone networks and physical infrastructure. A partial blackout affects part of the network (fixed or mobile), while leaving the rest operational.

Table 1. Types of digital shutdowns

[insert Figure 1.]

Between 2016 and 2019, the Internet experienced more than 590 shutdowns around the world, rising exponentially from year to year. In 2019 alone, the figure stood at 213 (Access Now, 2018; 2019). The most frequent justifications were: 1) the prevention of fake news and hate speech, 2) public safety and 3) national security. Nevertheless, Access Now states that the actual underlying reasons were, in fact: 1) political and religious demonstrations and protests, 2) military action, 3) political instability and communal violence and 4) elections. Internet shutdowns occurred both in autocratic,

hybrid[2] or failed states and in consolidated democracies. Internet blackouts are tested in the first group, to subsequently be implemented in relatively stable democracies, where they are becoming increasingly commonplace (Hintz and Milan, 2018).

Based on the above typology, 1-O involved an Internet shutdown in a democratic environment, combining first- and second-generation practices, implemented on both a preventive and reactive basis, giving rise to a partial blackout.

4. Justification, hypotheses and methodology

The referendum on October 1st 2017 in Catalonia was the outcome of the social and political groundswell taking place since 2010 and known there as the *procés* (process). Its stated goal was to express the Catalan public's position with regard to making Catalonia a sovereign state in the form of a republic. The complete opposition of those supporting national unity and the central Spanish authorities led to a growing identitary polarisation that pitted Catalonia's regional government –the *Generalitat*– against Spain's central government in Madrid. This conflict dominated the headlines and electoral agendas, clearly revealing two diametrically opposed public spheres (Almirón, 2018). Preparations for and the holding of 1-O –banned by the Constitutional Court– caused the judicialisation of this political conflict, up to and including at European level.

The events leading up to 1-O, as well as those of the day of the poll, reveal how the Spanish State implemented digital shutdown mechanisms in an attempt to prevent the public's participation in the referendum. This ended up being held, albeit with a police presence that attempted, unsuccessfully, to stop it. A total of 43.03% of the electoral roll "participated", 90.18% of whom voted "yes" and 7.83% "no"[3]. These figures from the *Generalitat* were not recognised by either Spain or the EU.

Mass civil disobedience (involving 2,286,217 voters) led to a unilateral declaration of independence, which was passed by a slender majority in the Catalan Parliament. This met with direct opposition from the Spanish Government. The temporary suspension of Catalan autonomy, the prosecution and subsequent imprisonment of twelve political and

[2] "Hybrid political regimes combine democratic elements –political pluralism, representative institutions, elections and/or constitutionalism– with authoritarian forms of power. Political competition may be restricted or a group with significant social support excluded. There may be political decision-makers who are not politically answerable, which limits the independence of representative institutions, and different forms of political rights and public freedoms may be restricted, despite being formally guaranteed" (Szmolka Vida, 2010: 115). Author's own translation.

[3] Generalitat de Catalunya: https://estaticos.elperiodico.com/resources/pdf/4/3/1507302086634.pdf

social leaders and the exiling of another eight parliamentarians exacerbated institutional tensions and protests in support of independence, which were markedly digital in nature.

The heuristic relevance of this case study lies in the following facts: a) It took place in an area where digital penetration levels are among the highest in Spain and the EU as a whole.. In 2018, 82.2% of Catalan citizens had digital connection in their homes and 88% were frequent Internet users[4]. b) The region has a widespread "hacktivist" movement (Fuster and Subirats, 2012) and an extensive associative network (Torcal et al., 2006) that takes a great advantage of digital technologies (Fuster and Spelt, 2019). c) The referendum received broad public support in Catalonia (70.8%), but only minority support in the rest of Spain (29.8% in favour versus 57.3% against)[5]. Lastly, d) the holding of 1-O was supported by 80% of Catalan local councils[6], and by the region's government and parliament, even though not of a clear majority of society or voters. Neither did it have a clear action plan, as would be shown subsequently (Antentas, 2019; Palà and Picazo, 2020).

We shall be testing three hypotheses:

H_1: The shutdown in Catalonia took place, involving the public administrations, central Spanish law enforcement and Spain's leading digital services companies.

H_2: Disintermediation thesis is refuted by the control over the Digital Public Sphere [DPS] exercised by the public administrations and digital corporations, which collaborated with the Internet shutdown either voluntarily (in exchange for favours) or under duress.

H_3: Catalan institutions and civil society implemented mechanisms to overcome the censorship and Internet shutdown imposed by the Spanish Government.

Our methodology triangulates bibliographical and documentary analysis with in-depth interviews. Given that the "procés" is both recent and complex, academic literature and empirical work are scarce. Additionally, a great deal of secrecy surrounds certain judicial decisions and police actions. We therefore review reports from independent organisations to indicate how the Spanish Government attempted to first impede and then interrupt the 1-O referendum. Said reports also help us understand the resistance strategies employed by civil society and the institutions supporting independence.

[4] IDESCAT, 2019. Survey on equipment and use of new technologies: https://www.idescat.cat/pub/?id=ticll18&n=1.1.1&lang=es

[5] *Centre d'Estudis d'Opinió* (CEO) 17/09/2019. Perception of the territorial debate in Spain: http://ceo.gencat.cat/ca/estudis/registre-estudis-dopinio/estudis-de-la-generalitat/detall/index.html?id=7368

[6] Wikipedia: https://en.wikipedia.org/wiki/Association_of_Municipalities_for_Independence

Additionally, we carried out two in-depth, semi-structured and open-answer telephone interviews with Nacho Amadoz, legal director at the fundacio.cat organisation, and Enric Pineda, *Pirates de Catalunya* (Pirates of Catalonia) coordinator at the time, both of whom were involved in the digital aspects of 1-O[7].

5. Analysis

We present below the players involved in 1-O and the dynamics of the control and blackout of the Internet. We note 1) the blocking of websites, 2) that of the online electoral roll, and 3) the partial shuttdown of the Internet. Lastly, we analyse the digital resistance offered by the Catalan independence movement.

5.1 The players

The Internet shutdown in Catalonia involved, directly or indirectly, a wide variety of individual and collective players (see Table 2). On the one hand, there were those attempting to restrict access to and block websites that provided assistance or support for the referendum; on the other hand, were those trying to keep them up and running and restore access to the Internet. In addition to the governmental players – the Spanish Government (in favour of the shutdown) and the *Generalitat* (against it) – there were Internet companies and providers, as well as civil society, which mobilised technical and human resources to keep digital communications operational.

Lastly, and outside of Table 2, there were Internet users who, as we shall see, employed –on a distributed basis– digital practices to hinder or facilitate the referendum. The degree to which these initiatives were independent is uncertain. The extent of the infiltration by Spanish police forces and the support provided by the *Generalitat* for the digital resistance before and after 1-O remains to be seen. The Spanish authorities attempted to interfere with the flow of communications and block digital content that supported the referendum. In this, in certain cases, it enjoyed the collaboration of Internet service providers[8]. Some companies began to cooperate after receiving court orders (e.g. Telefónica/Movistar, Vodafone, MásMóvil, Orange, C-Dom, and Google). Others were subject to coercive force, with the taking over of headquarters and bank accounts and the arrest of those refusing to obey court orders because they regarded

[7] Dates of interviews: Enric Pineda, 26/02/19; Nacho Amadoz, 03/03/2019.

[8] Qurium foundation documented how ISP Movistar collaborated with the central Spanish authorities to shut down websites: https://www.qurium.org/alerts/spain/blocking-techniques-catalunya/

them as arbitrary and unjustified (e.g. fundació.cat[9], T-Systems[10]). Other companies, despite receiving notifications, ignored them (e.g. Adamo, Parlem, Fibracat and Amazon). Small operators such as Parlem and Fibracat (both Catalan) used their own networks and circumvented the shutdown, meaning their users were always able to access the blocked sites. Given the judicial consequences and penalties associated, some of these companies did not specified if they failed to receive the official notification or simply disregarded it. However, this does show that a territory's ownership and management of its own digital service providers guarantees its digital sovereignty, at least to the extent of its competences.

Table 2. Key players in the shutdown in Catalonia

[insert Figure 2.]

Global technological corporations submit to the national law of territories in which they operate, as established in their service conditions. However, they enjoy more autonomy than they claim, as can be seen in our case study. Amazon, owner of the biggest "cloud" (digital repository), either refused to obey or "ignored", depending upon the source, the courts' shutdown orders. On the other hand, Google, its closest competitor, complied, although it later called for the suspension of the legal measures, considering them "disproportionate and unjustified"[11].

9 Fundació.cat is a private non-profit organisation whose funding depends exclusively on the management of the services it offers (sale and administration of the Internet domains .cat and .barcelona). It receives no kind of subsidy or public aid, as confirmed by Nacho Amadoz, head of the undertaking's legal services. Josep Masoliver, Head of Systems and Technological Innovation at fundation was the first to be arrested and accused of the offences of disobedience of authority, misappropriation of public funds and interfering with the administration of justice. https://el9nou.cat/tag/pep-masoliver/

10 T-Systems is a private German company that provides ICT management and supply services to Catalonia's Generalitat. According to a report from the Guardia Civil, the company was committed to the Generalitat to build and provide digital support for the state structure of the future digital Republic as well as computing support for the Referendum. Although the company denied these accusations, its vice president of services Rosa María Curto was arrested in her office at Madrid being accused of crimes of disobedience, embezzlement and prevarication. She was released after being required to desist from any activity that involved organizing the Referendum. https://www.lavanguardia.com/local/barcelona/20190304/46827852860/t-systems-niega-ilegalidades-tras-atribuirle-guardia-civil-participacion-en-el-1-o-o-crear-el-dni-de-la-republica.html

11 The TSJC ordered Amazon to block access to servers for the application so that Catalans abroad could register to vote, yet it was the only company not to comply. Google received a similar order to remove applications allowing people to vote. The company blocked access to up to eight domains linked to 1-O. Google LLC cancelled the Google Cloud service of the servers linked to the domains refloct.cat and refloct.eu, as well as those linked with certain domains (referendum.cat, ref.loct.cat, refl.oct.eu, refereum.ws and garantiespelreferendum.com). Six months later, in a letter to the TSJC, Google sought the lifting of the shutdown, arguing that it had a "disproportionate effect" and that its "definitive upkeep was unnecessary".

The different reactions of Amazon and Google seem to respond to decisions made in closed circles of power by the boards of directors. All indicates that Google sought not to harm its business relationships in Spain by disobeying legal decisions. While Amazon aimed to increase its corporate hegemony over cloud computing services (AWS) in a highly digitized territory, such as Cataluña, that planned to expand its digital infrastructures in the next decade[12].

5.2 The shutdown of websites

Alongside the seizure of signs and posters calling for the referendum, websites associated with it were also shut down. According to a report by Nodo50, an ISP for Spanish and Latin American social movements, a total of 70 were blocked[13]. Other sources estimate that 140 websites were closed by order of the High Court of Justice of Catalonia ("TSJC") (Moya and Coca, 2018). Nacho Amadoz of fundació.cat believes that the number ranges between 150 and 160. These included not only sites providing technical support for the referendum, but also many others simply in favour of 1-O.

The case of fundació.cat is important, since a large number of the sites shut down used its domains. The first court orders ordered it to block all sites dealing with the referendum. The organisation managed some 109,000 active domains, which had to be monitored to shut down those referring to the holding of 1-O. fundació.cat argued that this imposed unlawful censorship duties, with undefined and non-explicit criteria for blocking pro-independence websites (Amadoz).

fundació.cat complained before ICANN –the international organisation that allocates domain names and to which it belongs– that the judicial measures forced it to disclose customer information and shut down websites. Google filed a complaint before the Barcelona courts regarding the closure of the referendum website. And the Internet Society expressed concern about the shutdown of sites providing information on 1-O[14].

5.3 The blocking of the universal electoral roll systems and the "blackout" during 1-O

12 Amazon's business plans in Spain a decade after the referendum: https://elpais.com/tecnologia/2019/10/31/actualidad/1572543489_687316.html

13 Nodo50, sites closed during 1-O: https://www.nodo50.cat/lista.txt

14 Internet Society, 21/09/2017: https://www.internetsociety.org/news/statements/2017/internet-society-statement-internet-blocking-measures-catalonia-spain/

On 30 September 2017, two days before the referendum, Spain's *Guardia Civil* police force seized the Centre for Telecommunications and Information Technology (CTTI) and the Information Security Centre of Catalonia (CESICAT), the two regional bodies responsible for counting and checking votes. In reaction to their shutdown, the *Generalitat* hosted the universal electoral roll and a digital authentication service on Amazon servers. In the morning of October 1st, the "registremeses.com" website was shut down[15]. "Registremeses.com" was the domain that hosted the application containing the universal census. Through this website, and as Minister Raül Romeva explained in the previous days of the 1-O, any "Catalan citizen could vote at any "electoral college"[16].

During 1-O, the *Guardia Civil* tried to "block this *universal electoral roll* so that polling stations could not check whether voters were registered or had already voted"[17]. Attempts to shut it down also came from outside of Spanish law enforcement bodies. The electoral roll's site suffered from a distributed denial-of-service attack (DDoS)[18] coordinated from the *ForoCoches* website by an anonymous user, Alextango, who asked for help on this forum. The Qurium foundation raised the possibility that the police monitored the process using DPI (Deep Packet Inspection) technology[19].

Internet shutdowns were experienced in many Catalan towns and cities. Numerous media outlets, some aggressively opposed to the Catalan independence movement[20], stated that the Catalan Ministry of Education's network was shut down to prevent connection with schools that had been converted into polling stations. This network, run

15 Websites are hosted on servers using numerical "IP" (Internet Protocol) addresses. The DNS (Domain Name System) associates these IP addresses with a specific name. This is how one accesses a server hosting a website with a specific domain name. On 1-O, it was not possible to access the site using the domain name *registremeses.com*. To do so, you had to know the site's numerical IP address.

16 https://www.eitb.eus/es/noticias/politica/detalle/5115536/referendum-catalan-1-octubre-implantado-censo-universal/

17 *El País*, 09/09/2017: https://elpais.com/politica/2017/10/09/actualidad/1507541168_944893.html

18 Wikipedia: "a denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet". https://en.wikipedia.org/wiki/Denial-of-service_attack

19 Qurium: https://www.qurium.org/alerts/spain/blocking-techniques-catalunya/ Deep Packet Inspection: this technology permits access to specific users' flows or information and the inspection of their communications in detail, without being the recipient of the data packets.

20 *El Confidencial*, 04/10/2017: https://www.elconfidencial.com/tecnologia/2017-10-04/referendum-supera-bloqueo-informatico_1454677/

by Telefónica, provided the service to Catalonia's education centres. As Carlos Bajo notes:

> Everything seems to indicate that an Internet shutdown operation took place in a wide number of points, […] when, on 29 September, the High Court of Justice of Catalonia ordered the suspension of any computer services facilitating voting via the Internet[21].

The Internet shutdown/blackout involved both institutional players and private telecommunications companies, with different inclinations and degrees of independence, as we first hypothesized. Additionally, the shutdown was performed, as usual (Hintz and Milan, 2018), in an opaque way to avoid accountability. This confirms our second hypothesis: digital disintermediation is placed in doubt by diverse dynamics of state and corporate control.

Limited time and resources, not to mention scant cooperation from the actors involved, who refused to be interviewed, have prevented a more in-depth analysis. This would examine, amongst other things, possible business favours, such as the cancelling of a 26 million-euro fine against Telefónica by Spain's *Audiencia Nacional* (National High Court) in the days prior to the referendum[22]. In our conclusions, we outline and deepen some possible future research lines.

5.4 Digital resistance practices within the framework of 1-O

Lastly, we tackle the digital resistance displayed by the *Generalitat* and/or by pro-independence civil society. It has proven difficult to make a clear distinction between these two players, even for media critical of the Spanish Government[23].

To counter the shutdown of domains and sites, begun in the weeks running up to 1-O, members of platforms such as *Pirates de Catalunya* voluntarily decided to upload mirrors of the referendum website to their personal portals. They then uploaded to the Internet an instruction manual showing others how to replicate the action. Following hacker ethics (Himanen, 2001), they shared their skills in support of free digital access.

[21] *El Salto*, 22/04/2018: https://www.elsaltodiario.com/cataluna/apagar-red-control-internet-referendum-catalunya. Author's own translation.

[22] *Ara.cat*, 07/09/2017: https://www.ara.cat/economia/justicia-anulla-Competencia-Telefonica-milions_0_1865213626.html

[23] *Viento Sur,* 28/12/2019: https://vientosur.info/spip.php?article15462

Enric Pineda, then coordinator at *Pirates de Catalunya*, claimed that they mirrored the referendum site "because it only promoted a democratic procedure". They regarded the shutdown as an arbitrary act and a restriction on political liberties and free speech. Pineda states his decision was not motivated by any link with the *Generalitat* or financial gains. He felt that he was helping "civil society to take control over the political and social process experienced by Catalonia in recent years". Organisations such as Alerta Solidaria and The Pirate Bay, amongst others, also mirrored the blocked sites. They were also shared by pro-independence civil and cultural organisations such as *Òmnium Cultural* and the *Assemblea Nacional Catalana* (ANC), who saw how Spanish Internet companies also blocked their sites. These organizations and civil society used proxies[24] to access pro-independence blocked websites using external servers.

During 1-O, to counter the attacks on the IPs hosting the universal electoral roll, the *Generalitat* provided an instruction sheet and a hotline for communicating with polling stations. The hotline was used for notifying incidents and for telling polling stations how to access the digital electoral roll.

Additionally, some Catalan hacktivists carried out attacks on the *ForoCoches* portal during 1-O. As already noted, *ForoCoches* coordinated the DDoS on the electoral roll's IPs. Profiles such as AnonymousBCN blocked *ForoCoches* on the afternoon of October 1st, preventing attacks on the voters' register sites. The confrontation and polarisation between "unionist" and pro-independence Internet users thus took on a digital dimension. Unionists used *ForoCoches*, one of the 100 most-visited sites in Spain that allows to create threads on any subject. The independence movement, for its part, enjoyed the support of the Barcelona chapter of Anonymous, hacktivism's most belligerent (albeit hidden) face. More institutionalised hacker circles, such as the Pirate Party and its international network, also backed the 1-O.

To protect connections with polling stations, voters themselves and referendum volunteers shared mobile data to retain access to the electoral roll. They thus acted as "recursive publics" (Kelty, 2008), using their mobile devices to complement the digital infrastructure. The 3G and 4G mobile networks were, in many cases, the only way of connecting to the Internet. Although this slowed down the voting process and made it more unwieldy, it helped to circumvent (in part, at least) the shutdown in different areas. Additionally, communication tools such as FireChat were activated. Since they work via Bluetooth, they do not require Internet. Using mesh networking, such apps allow users to communicate with any device within the net created with mobile phones.

Lastly, leading digital rights organisations (Xnet, Access Now, the Electronic Frontier Foundation, etc.) denounced the shutdown and the blackout of the DPS that took place

[24] A proxy service acts as an intermediary between a user's device and the server upon which the contents he or she wishes to access are hosted.

in Catalonia[25]. Ruling 459/2019 of the Spanish Supreme Court on 1-O led to collective digital resistance launched by the so-called *Tsunami Democràtic* [*TD*]. This mass, non-violent civil disobedience platform sprang from the 1-O initiatives that had, over the course of September and October 2017, safeguarded 8,000 ballot boxes without them being discovered by either Spain's police or Secret Service[26]. The *Audiencia Nacional* ordered the closing down of *TD*'s website and its social network profiles, accusing it of an alleged act of terrorism[27].

TD organised mass blockades of both Barcelona's airport and the border with France. It also held other, albeit less successful, actions at other popular events. It leveraged peer-to-peer (P2P) and blockchain technology to create a network in which all nodes were connected and in which the shutdown of one would not compromise the entire system. It also followed the model used by the protestors in Hong Kong organising simultaneous actions against the Chinese Government. Geolocating the activities allowed members to be called to action based on their proximity. *TD* also innovated, requiring face-to-face contact and the scanning of a QR provided by a trusted person for installation of the app (Scolari, 2019).

TD's Telegram account registered over 400,000 followers by the last week of January 2020, but its page remained suspended by "order of the judicial authorities"[28]. Despite the distributed nature of *TD*, its convergence with the approaches and timetables of pro-independence parties and organisations called into question its independence[29]. This leads to an interesting aspect of distributed, anonymous hacktivism, also noted in the possible police infiltration against pro-independence sites in the DDoS attacks coordinated on *ForoCoches*. Digital anonymity increases effectiveness, but obfuscates who is behind them and blurs responsibility arising therefrom. The possible involvement of the Spanish police in the digital "unionism" and of the *Generalitat* in the

[25] Xnet, 21/09/2017: https://xnet-x.net/democracia-derechos-y-libertades-catalunya-caso-estudio/
Electronic Frontier Foundation, 21/09/2017: https://www.eff.org/deeplinks/2017/09/cat-domain-casualty-catalonian-independence-crackdown
Access Now, 02/10/2017: https://www.accessnow.org/cameroon-spain-network-shutdowns-interference-violence-erupts/

[26] *eldiario.es,* 15/10/2019: https://www.eldiario.es/catalunya/politica/trabajo-intentar-colapsar-aeropuertos-Tsunami_0_952955003.html

[27] See this description of *Tsunami Democràtic* as non-violent in a newspaper whose editorial line opposed the independence process. *El Pais*, 11/11/2019: https://elpais.com/politica/2019/11/11/actualidad/1573463539_877025.html

[28] Original *TD* web domain: http://82.223.97.47/ Active mirror: https://tsdem.gitlab.io/

[29] *Viento Sur,* 28/12/2019: https://vientosur.info/spip.php?article15462

independence movement points to the potential inroads of state control into Internet activism's cutting edge.

Despite uncertainties, the digital resistance strategies identified confirm the third hypothesis raised. The Spanish State and the digital companies' shutdown found resistance in civil society, which carried out actions to circumvent the censorship and maintain their digital autonomy, as well as the 1-O referendum's infrastructure, despite being hit by the police and the judiciary.

Lastly, it is worth highlighting the wish of Catalan institutions to develop a "digital republic", inspired by self-determination processes such as that of Estonia[30]. These still experimental experiences conceive digital ICT as tools for creating or maintaining state structures amidst institutional conflicts. They entail civil society's involvement in the building and defence of communications scenarios that can later become territorial in nature.

The aim of this so called Digital Republic was for Catalan "cyber-society" to adopt a collective civic identity, freely and voluntarily adhered to. The response of the Spanish State was to make it unworkable. The (then caretaker) government of Pedro Sánchez (PSOE) passed Royal Decree-Law 14/2019, of October 31st 2019, which permitted the closing down of websites and limiting Internet access without a court order. It thereby overcame the need for the support of telecommunications operators, as had been the case with 1-O. The new legislation entailed a great degree of uncertainty and a restriction of legal rights, creating a deterrent effect. The Royal Decree 14/2019 proved an evolution from applying existing legal instruments to setting specific digital regulations which in this case undermined democratic rights and pluralism as the judicial literature warned both at the Spanish (Teruel, 2014) and European levels (Monti, 2019; Parti and Marin, 2013).

6. Discussion and conclusions

2017's "1-O" revealed how an internationally recognised democratic regime's DPS can be interfered with through cooperation between state power and technology companies. The notion of digital disintermediation is a myth. The Catalan independence referendum aimed to break national unity and install a republic. There is no doubt that both of these goals lie outside the framework of Spain's Constitution. However, some actions of the Spanish government may not have respected the political freedoms and civil liberties recognised by the same Constitution. Their continuing enforcement over time even less so. That is why some associations in defence of press and digital rights asked the *Defensor del Pueblo*, Spain's ombudsman, to make an appeal to the Constitutional

[30] *ElNacional.cat*, 25/11/2018: https://www.elnacional.cat/es/politica/estonia-republica-inspira-catalunya_328347_102.html

Court against Royal Decree 14/2019, which allows Internet shutdowns without court orders[31].

The 1-O shutdown affected a significant number of websites that, far from fostering hatred or infringing upon human rights, merely promoted a referendum. To prevent it, platforms facilitating online voter registration and actual voting were censored. But this censorship affected domains that were simply expressing political opinions and positions. To the extent that they were promoting a banned action, their censorship could be viewed as preventing a crime. Nevertheless, as these webs were not inciting violence, this could also be considered an infringement of political freedoms on the Internet[32]. Alleged violations extended beyond the digital domain with arrests, searches and court orders of dubious lawfulness. Equipment and facilities were seized with both physical and psychological violence, again documented by recognised international bodies (Moya and Coca, 2018). Instead, other authors provide a legal justification of the measures taken by the Spanish state "to defend the Constitution against secessionism" (Azpitarte, 2018) .

Òmnium Cultural calculates the number of those affected on or after 1-O at 1,396 injured and 292 arrested by Spanish state law enforcement[33]. The total figure stands at 2,500 people convicted and/or investigated. The same organisation documented 144 websites closed and 18 people investigated for mirroring the referendum site. These latter figures match those of other sources noted in this article. Human rights NGO and digital freedom organizations together issued reports denouncing the reaction of the Spanish state.[34]

Amnesty International also documented the excessive use of force by the police on 1-O and complained that the conviction for sedition of two activists, Jordi Sànchez and Jordi Cuixart, violated the rights to free expression and peaceful protest[35]. Amnesty International blamed their jail sentences and those of another seven leading politicians

31 These were: *Plataforma en Defensa de la Libertad de Información*, the *Asociación de Internautas*, the *Asociación de Usuarios de Internet*, *FACUA-Consumidores en Acción*, *Grupo 17 de Marzo* and *Críptica*: http://libertadinformacion.cc/el-defensor-del-pueblo-estudiara-la-posibilidad-de-recurrir-ante-el-constitucional-el-decretazo-digital/

32 Nacho Amadoz, (fundació.cat) stated that the court order asked them to block all .cat domains containing any information on the referendum. This order, he warned, was "very ambiguous, vague and dangerous […], and it imposed upon as a burden of censorship that we regarded as unlawful […] If we had complied with that order to the letter, we would have had to have blocked all websites talking about the referendum, including those of the media", adding: "were we supposed to shut down only those sites speaking out in favour of the referendum or also those against it?". Author's own translation.

33 *Òmnium Cultural*, 17/12/2019: https://twitter.com/omnium/status/1206893799580061696

34 http://libertadinformacion.cc/herramientas/observatorio-1-o/

35 Amnesty International, 19/11/2019: https://www.es.amnesty.org/fileadmin/user_upload/DeclaracionPublica_191119_FINAL.pdf

on a "vague definition of the crime of sedition". "Jordi Sànchez and Jordi Cuixart must be released immediately and their convictions on the charge of sedition must be quashed", stated Daniel Joloy, Senior Policy Advisor at Amnesty International[36]. For its part, the UN's Human Rights Council included Spain in the Universal Periodic Review (UPR) to verify possible transgressions of international human rights conventions. Along the same lines, and again leveraging online practices, March 2019 saw the start of a campaign of citizens' self-incrimination[37], a precursor to that promoted by *Òmnium Cultural* after the issuing of the conviction ruling[38]. The Internet shutdown followed other actions aimed at discrediting the Catalan independence movement in previous years, a leading example of which was *Operación Cataluña*, a set of actions Spain's by which the Interior Ministry tried to discredit the Catalan *procés*. This became a media *affaire* uncovering several manufactured scandals against pro-independence leaders[39].

The clash between Spain's central government and Catalonia's *Generalitat*, as well as the news coverage given by Madrid and Catalan media outlets, had created territorialised and opposing public spheres some time previously[40]. The Spanish State public sphere depicted an antagonistic conflict, whilst the Catalan public sphere –even anti-independence media outlets– put their weight behind a solution based on dialogue (Almirón, 2018). 1-O laid bare the polarisation between the two public spheres and the two opposing digital dynamics (Sampedro et al., 2018).

The Spanish State attempted to control the flow of information on a centralised and hierarchical basis. To legitimise its restrictions, it used two arguments. One was obvious: both the referendum and the subsequent declaration of independence were illegal. The other was more typical of unstable democracies or authoritarian regimes: the *procés* was also the result of a foreign interference in national sovereignty. In this case, the finger was pointed at Wikileaks and at "Russian and Venezuelan hackers", without any empirical evidence whatsoever[41]. This narrative framework legitimised the curtailing of digital sovereignty in Catalonia in the name of Spain's national sovereignty. Using as its basis national jurisprudence, the Spanish State attempted to

[36] Amnesty International, 19/11/2019: https://www.amnesty.org/en/latest/news/2019/11/spain-conviction-for-sedition-of-jordi-sanchez-and-jordi-cuixart-threatens-rights-to-freedom-of-expression-and-peaceful-assembly/

[37] *Público*, 23/04/2019: https://blogs.publico.es/dominiopublico/28487/por-que-nos-autoinculpamos-con-los-jordis/

[38] *Òmnium Cultural*: https://hotornaremafer.cat/autoinculpacions/

[39] Público TV: *Las cloacas de Interior*: https://www.publico.es/videos/624801/las-cloacas-de-interior-el-documental-completo

[40] Hierro (2012) analyses the role of the Catalan media and public television in shaping the Catalan national identity. Sampedro and Duarte (2008) reveal the hidden agenda of the Madrid press in 2004 regarding the alleged connivance of the Catalan independence movement with ETA, prior to the "11M" terrorist attacks. Valera (2018) shows a clear audience segmentation based on national identities, meaning that people with Catalan nationalist inclinations prefer to consume regional media, whilst non-nationalists prefer Spain-wide media. Lastly, see the special edition of the *Catalan Journal of Communication & Cultural Studies,* 2019*,* vol. 11, no. 2 on the media and digital-related aspects of the "Catalan conflict".

[41] *Público*, 15/11/2017: https://www.publico.es/politica/teoria-conspiracion-hackers-rusos-venezolanos-enemigo-forma-simulacion.html

maintain the rule of law and exercised its monopoly on physical and digital violence, implementing first- and second-generation control measures. With both selective and random repression mechanisms, the "unionist" discourse prevailed, aided by the high degree of parallelism between the Spanish media establishment and its political system (Büchel et al., 2016). Acquiring as it did the nature of a law, the shutdown of the Internet on 1-O led to a setback for digital rights and freedoms throughout Spain as a whole.

By way of contrast, the Catalan Government and pro-independence civil society (or those in favour of holding the referendum) attempted to circumvent the Internet shutdown. In the weeks leading up to 1-O, Catalonia's institutional channels were overwhelmed. Pro-independence organisations and individuals supporting the referendum maintained – not without difficulties – the digital flow of information. This defence of rights and freedoms was carried out in a collaborative and distributed manner, despite the authorities' (Spanish and Catalan) attempts to interfere in the process.

7. Future analysis

In the light of this study, we suggest that future research on this or other Internet shutdowns should examine the three poles of digital political information. In that of the *public administrations*, at least these factors are important: the framework legislation on digital rights and markets, the government's ideological orientation, its capacity for political and parliamentary action based on the consensus it achieves, the collaboration of the judiciary, law enforcement and the authorities in the areas in which the shutdown is implemented, as well as the discourse it seeks to impose and its support amongst the general public.

In that of *companies*, it is important to take into account whether they are domestic or foreign and hence the legal framework in which they are acting. However, it appears even more important to consider whether they have their own infrastructures. Also of significance are the international trading agreements between countries and supranational bodies. Besides, one should not forget the amount of business and any contracts between these companies and the public administrations, as well as their plans for business growth. It is also important to remember the legal teams available to the corporations, their prior "form" and that of their competitors in similar cases, the reactions of their management and staff and their business codes of conduct.

This list of variables to be examined is by no means exhaustive. Upcoming studies should also look at the end-user licence agreements for apps and technological services used by *'netizens*. These represent the third pole of political communications and supposedly assume before the companies a code of conduct, associated with the rights the companies should safeguard. Internet users should be able to demand enforcement

of these rights and, obviously, use other technologies and their own infrastructures, without unjustified corporate or state control or interference. The level of digital competence of the affected population and the extent of their organisation into Internet user associations are other important variables to be borne in mind in future research work.

References

Access Now (2018) 'The state of internet shutdowns around the world 2018' [online], available in: https://www.accessnow.org/cms/assets/uploads/2019/07/KeepItOn-2018-Report.pdf, retrieved: 10/02/2020.

Access Now (2019) 'The #KeepItOn report on internet shutdowns in 2019' [online], available in: https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf, retrieved: 05/03/2020.

Almirón, Nuria (2018) ''Go and get'em!': Authoritarianism, Elitism and Media in the Catalan crisis'. The Political Economy of Communication 6(2): 39-73.

Antentas, Josep (2019) Espectros de octubre [October's wraiths]. Barcelona: Sylone.

Beltrán, Natalia (2016) 'Technological sovereignty: what chances for alternative practices to emerge in daily IT use?'. Revue Hybrid 3: 1-20.

Benkler, Yochai, Robert Faris, Hal Roberts and Ethan Zuckerman (2017) 'Study: Breitbart-led right-wing media ecosystem altered broader media agenda' [online], available in: https://www.cjr.org/analysis/breitbart-media-trump-harvard-study.php, retrieved: 09/02/2020.

Büchel, Florin, Edda Humprecht, Laia Castro-Herrero, Sven Engesser and Michael Brüggemann (2016) 'Building empirical typologies with QCA: Toward a classification of media systems'. International Journal of Press/Politics 21(2): 209-232.

Castells, Manuel (2009) Communication power. New York: Oxford University Press.

Couldry, Nick and Andreas Hepp (2016) The Mediated Construction of Reality. New Jersey: Wiley.

Fenton, Natalie (2016) 'Left out? Digital media, radical politics and social change'. Information, Communication & Society 19(3): 346-361.

Freedom House (2017) 'Manipulating social media to undermine democracy' [online], available in: https://freedomhouse.org/sites/default/files/FOTN_2017_Final.pdf, retrieved: 10/02/2020.

Fuster, Mayo and Joan Subirats (2012) Més enllà d'Internet com a eina 'martell' - eina de la vella política: Cap un nou Policy Making? [Beyond the Internet as a 'hammer' tool - an old policy tool: Towards a new Policy Making?]. Barcelona: Universitat Autònoma de Barcelona.

Haché, Alex (2014) 'Technological sovereignty'. Mouvements 79(3): 38-48.

Haché, Alex (2017) 'Technological Sovereignty: Learning to love machines again', in Spideralex (ed) Technological Sovereignty, Vol. 2 [online], available in: https://sobtec.gitbooks.io/sobtec2/en/content/02intro.html, retrieved: 16/03/2020.

Hierro, María José (2012) 'Changes in national identification: A study of the Catalan case', PhD Dissertation, Madrid, Universidad Autónoma de Madrid.

Himanen, Pekka (2001) La ética del hacker y el espíritu de la era de la información. Barcelona: Destino.

Hintz, Arne and Stefania Milan (2018) ''Through a Glass, Darkly': Everyday Acts of Authoritarianism in the Liberal West'. International Journal of Communication 12: 3939-3959.

Kelty, Christopher (2008) Two Bits: The Cultural Significance of Free Software. Carolina del Norte: Duke University Press.

Marwick, Alice and Rebecca Lewis (2017) Media Manipulation and Disinformation Online. New York: Data & Society Research Institute.

Michaelsen, Marcus and Marlies Glasius (2018) 'Authoritarian Practices in the Digital Age'. International Journal of Communication 12: 3788-3794.

Moya Manzano, Patricia and Juan Coca (2018) 'Estados vs. Hackers: El cierre de la Esfera Pública digital y el proceso en Cataluña' [States vs. Hackers: The shutdown of the Digital Public Sphere and the process in Catalonia], Final Degree Project, Madrid, Universidad Rey Juan Carlos.

Palà, Roger and Sergi Picazo (2020) Catalunya: un moment crític [Catalonia: a critical moment]. Barcelona: Rosa dels Vents.

Perales-García, Cristina and Carles Pont-Sorribes (2018) 'The Spanish-Catalan political crisis as represented in the UK, French and German press (2010-2017)'. Essachess. Journal for Communication Studies 11 2(22): 147-162.

Rheingold, Howard (2002) Smart Mobs: The Next Social Revolution. New York: Basic Books.

Sampedro, Víctor and José Manuel Sánchez-Duarte (2008) 'Pre-campaña y gestión de la agenda electoral. Carod Rovira y la tregua catalana de ETA' [Pre-campaign and management of the electoral agenda. Carod Rovira and the ETA's truce in Catalanonia], pp. 29-78 in V. Sampedro (ed.). Medios y elecciones 2004 [Media and elections 2004]. Madrid: Centro de Estudios Ramón Areces.

Sampedro, Víctor, F. Javier López-Ferrández and Álvaro Carretero (2018) 'Leaks-based journalism and media scandals: From official sources to the networked Fourth Estate? European Journal of Communication 33(3): 255-270.

Scolari, Carlos (2019) '#TsunamiDemocràtic: las nuevas interfaces políticas en la era de Blockchain' ['#TsunamiDemocràtic: the new political interfaces in the Blockchain era] [online], available in: https://hipermediaciones.com/2019/10/17/tsunamidemocratic-blockchain/, retrieved: 09/02/2020.

Shirky, Clay (2010) Cognitive Surplus: Creativity and generosity in a connected age. New York: Penguin.

Splichal, Slavko (ed) (2019) The Liquefaction of Publicness: Communication, Democracy and the Public Sphere in the Internet Age. London: Routledge

Striphas, Ted (2015) ‘Algorithmic culture’. European Journal of Cultural Studies 18(4-5): 395-412.

Szmolka Vida, Inmaculada (2010) ‘Los regímenes políticos híbridos: Democracias y autiritarismos con adjetivos’ [Hybrid political regimes: Democracies and autiritarisms with adjectives]. Revista de Estudios Políticos 147: 103-135.

Torcal, Mariano, Joan Font Fábregas and José Ramón Montero (eds) (2006) Ciudadanos, asociaciones y participación en España [Citizens, associations and participation in Spain]. Madrid: CIS

Valera, Lidia (2018) Medios, identidad nacional y exposición selectiva: predictores de preferencias mediáticas de los catalanes [Media, national identity and selective exposure: predictors of media preferences among the Catalan population]. Revista Española de Investigaciones Sociológicas 164: 135-154.

Van Dijk, José (2014) ‘Datafication, Dataism, and Dataveillance: Big Data Between Scientific Paradigm and Ideology’. Surveillance & Society 12: 197-208.