Data activism versus algorithmic control. New governance models, old asymmetries

El activismo de datos frente al control algorítmico. Nuevos modelos de gobernanza, viejas asimetrías

Paz Sastre Domínguez
(Universidad Autónoma Metropolitana) [p.sastre@correo.ler.uam.mx]

Ángel J. Gordo López
(Universidad Complutense de Madrid) [ajgordol@ucm.es]

DOI: https://dx.doi.org/10.12795/IC.2019.i16.04

E-ISSN: 2173-1071 IC – Revista Científica de Información y Comunicación
2019, 16, pp. 183 - 208

Abstract

This paper discusses the notion of algorithmic governance and data activism with examples that illustrate the emergence of new governance models in different countries. With the selection and brief analysis of the discourse of specific projects, the aim is to offer an overview that supports and encourages research and debate on how old asymmetries linked to the exercise of citizenship have repositioned themselves in the 'Age of Algorithms'.

Resumen

El artículo discute la noción de gobernanza algorítmica y de activismo de datos con ejemplos que ilustran la aparición de nuevos modelos de gobernanza en diferentes países. La selección y el análisis sucinto del discurso de proyectos específicos pretende ofrecer un panorama amplio que apoye y fomente la investigación y el debate sobre cómo se reposicionan las viejas asimetrías ligadas al ejercicio de la ciudadanía en la «era de los algoritmos».

Keywords

Algorithmic governance, data activism, open data, dataveillance, blockchain, technological solutionism.

Recibido: 15/06/2019
Aceptado: 23/09/2019

IC – Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208] E-ISSN: 2173-1071

Palabras clave

Gobernanza algorítmica, activismo de datos, datos abiertos, vigilancia de datos, blockchain, solucionismo tecnológico.

Summary

Sumario

E-ISSN: 2173-1071 IC – Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208]

1. Introduction

Snowden's disclosures regarding the global surveillance performed by the United States on the Internet in 2013 and the Cambridge Analytica scandal in 2018, linked to Facebook's advertising services, brought to light the use and abuse of data by companies and governments to influence public deliberation and conflict resolution processes at a global level. There has been much debate in Europe on whether or not the formulation of the new General Data Protection Regulation (GDPR) includes a 'right to an explanation', which would make it obligatory to inform users about what algorithms are doing with their data (Selbst & Powles, 2017). While in Spain, the Constitutional Court recently overturned the draft bill presented by the Spanish Socialist Workers' Party (PSOE), backed by the People's Party (PP), to use databases with an ideological profile for marketing campaigns. The intention of the draft bill was to legalise the automated submission of customised electoral messages to the contacts of constituents without their prior consent (*El Minuto Político*, *El diario.es*, 2019) (see also Europa Press, 2018).

The scandals that have rocked the public and private information and communication technology (ICTs) sectors have exacerbated even more the problems of representation, participation, legitimacy and hegemony that parliamentary democracies have been attempting to tackle for some time now (Habermas, 1976; Hall, Critcher, Jefferson, Clarke, & Roberts 1978). The news seems to have converted crime into the chief dilemma nowadays. As Lea (2002) notes, since the end of the twentieth century criminalisation has become the management model for socioeconomic problems, in addition to having totally displaced social policies. In current capitalism, crime acts as a key form of economics in which the rising crime rate in all social sectors provides the ideological justification for implementing new control mechanisms.

Notwithstanding the alarm bells, in this context the 'datification' and automation of governance procedures seems implacable. The increasingly greater volume of data surpasses our interpretation capacity, thus making us more and more dependent on the mathematical models required for their analysis. The potency of these model has led authors such as Rainie and Anderson (2017) to dub the present moment the 'Age of Algorithms'.

IC – Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208] E-ISSN: 2173-1071

Algorithms oil the wheels of computer apps with predetermined sequences of steps to be followed to produce, manage, analyse and interpret massive data sets. This information is then used to fuel the artificial intelligence (hereinafter AI) of expert systems that indicate, for example, what to buy, the shortest route, how to invest, what news to read, who can be a better employee or the ideal couple, the most adequate sentence, the illnesses that we will suffer in the future, the cheapest hotel, if we are eligible for a loan or for whom to vote, among many other things.

The aim of these expert systems is to anticipate and control individual behaviour. To this end, a sort of engineering of individual behaviour, a 'generalized digital behaviourism', as Rouvroy and Berns (2013) label it, has been designed on a vast scale. These would then be new forms of authoritarianism that dispense with public deliberation on issues pertaining to the representation, participation, legitimacy and hegemony inherent to citizenship.

The roles that the state has traditionally played to guarantee social order now have a competitor in the new algorithmic governance paradigm. The 'datification' and automation of procedures relating to decision-making and conflict resolution in all imaginable spheres of life not only imply new control and surveillance techniques guaranteeing the planned obsolescence of the citizenry, but have also paved the way for new forms of activism.

Data activism explores how the vast amount of data and information that we generate online have not only resulted in new forms of control and social surveillance, but also in new challenges and opportunities for the citizenry. Milán and Gutiérrez (2015) understand data activism as a new manifestation of citizen media, in which people and organisations give meaning to complex information employing software that allows for the circulation and management of that same information, central to civic actions aimed at social change.

But this is not the only possible interpretation. Data activism can be seen as a reaction to the new algorithmic control techniques that are challenging the very foundations of citizenship. Through a number of examples, our intention here is to illustrate the reactions of data activism to the emerging forms of authoritarianism. By briefiy analysing the discourse of activists on the intensive use of socially distributed information systems, the idea is to show how new alternative governance models, and not only new citizen media, have appeared.

E-ISSN: 2173-1071 IC – Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208]

First and foremost, the intention is to discuss the notion of algorithmic governance on the basis of a review of some of the recent theoretical approaches. Secondly, the reactive and proactive modalities of data activism are described, on the basis of the work of Milán and Gutiérrez (2015). The characteristics of algorithmic governance and the differences between the reactive and proactive sub-groups organise the analysis of the discourses linked to specific data activism projects that demonstrate the advent of new governance models in different countries. It should be noted that they are not exhaustive studies and that they were selected on the basis of our own personal experiences and on a previous study of environmental criminology (Sastre, 2019, in press). The purpose is to offer an overview that supports and promotes research and debate on how the old asymmetries linked to the exercise of citizenship have repositioned themselves in the 'Age of Algorithms'.

2. Algorithmic governance

'Datification' has replaced the information stored in old state archives with large data centres located in the cloud, where social activity is monitored with sophisticated algorithms capable of identifying patterns and anomalies. Only algorithms can analyse the constant and random accumulation of digitised information from metadata, which summarise basic information about data. Apparently, the study of any phenomenon, including stock exchanges, earthquakes, the climate, viruses, neurons, consumption, emotions and even crime, can be reduced to algorithmically assisted datamining and analysis.

In his work on the socio-political implications of big data-based algorithms designed for crime prevention and control, Pasquinelli (2016) speaks of the emergence of an 'algorithmic governance' in contemporary computational capitalism. To his mind (2016, p. 252), the rules for social behaviour are 'no longer constructed through the archives of institutional knowledge but mathematically computed from below'. Data acquire scope, colour, volume, depth and meaning. They are integrated into 'new landscapes of knowledge that inaugurated a vertiginous perspective over the world and

IC – Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208] E-ISSN: 2173-1071

society as a whole: the eye of the algorithm, or algorithmic vision' (Pasquinelli, 2016, p. 250).

This perspective intrinsic to military drones runs the risk of detecting patterns in meaningless random data in very different contexts. The over-identification of patterns, 'false alarms' or false positives, known as 'apophenia', offers us a glimpse of the logic of the algorithmic vision that, according to Pasquinelli (2016, p. 255), 'it would be more correct to call [...] Pattern Police'.

Apps aimed at 'preventive police action', such as PredPol, CompStat and HunchLab exemplify the algorithmic vision characterising new governance techniques. Based on seismic monitoring software, PredPol observes crime in an area, incorporates it into historical data and, by identifying spatial patterns, predicts when and where it might reoccur. The programme processes the data and calculates, hour after hour, where there are going to be hotspots in the immediate future, streamlining the distribution of city patrols, under the promise of scientifically optimising police work, cutting costs and improving results by reducing the street crime rate. E. Morozov (2015, p. 182) presents it as the epitome of technological solutionism when asserting that '[...] there is hardly a better example of how technology and big data can be put to work to solve the problem of crime by simply eliminating crime altogether'. Similarly, on the role that Dick (2002 [1956]) assigned the Precrime police division and the Precognitives in his short story adapted to the big screen by Spielberg (2002), Morozov (2013, p. 182) wonders, 'who wouldn't want to prevent crime before it happens?'

Computational operations, apparently lacking subjective bias, are replacing human intervention. However, it has been widely demonstrated that algorithms and data reproduce old asymmetries of race, class and sex (Angwin, Larson, Mattu, & Kirchner, 2016; Pishko, 2014; Rosenblat & Stark, 2016; Dastin, 2018). O'Neil (2016) illustrates how algorithmic governance systems include the same prejudices and biases present in society in their calculations. Even so, the proposal to perform regular and independent algorithmic audits has not caught on. The vast majority of 'clouds' and algorithms are still opaque and closed to public scrutiny (Morozov, 2013; Tutt, 2017).

In the United States, more than 20 states use risk assessment programmes based on data analysis, most of which are proprietary software

E-ISSN: 2173-1071 IC – Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208]

packages whose exact methods are still a mystery, to determine which people are more likely to be repeat offenders (Pishko, 2014). These programmes promise to reduce the prison population, without endangering the citizenry, under the pretext of the transparency and objectivity of techno-scientific by-products. Although a 'side' effect of this 'preventive police action' is the general criminalisation of the socially excluded.

In this respect, and in line with Shuttleworth and Moglen (2018) and Nadal and De la Cueva (2012), sometime ago it was proposed that the source code (the programming governing the functioning of software) and algorithms should belong to everyone, without being subject to copyrights, as with the law and case law. For De la Cueva (2019, in press), the technological sovereignty of a state depends on its transparency as regards the source code of the programmes used for management and control tasks. Hence the importance of promoting 'legal rules that establish which bodies have the authority to write source codes and algorithms—to which us citizens should also have access—in addition to the procedures governing their functioning' (De la Cueva, 2019, in press). Following this line of argument, preventing access to the source code of traffic lights, speed radars or the programmes that manage and administer legal rulings that might have resulted from the application of some or other software, is tantamount to ignoring that the 'technological sovereignty of a state rests precisely on its capacity to act transparently with respect to the source code of programmes used for undertaking management and control tasks' (De la Cueva, 2019, in press).

The sheen of transparency and objectivity of algorithmic governance does not only derive from the growing volume of data relating to our behaviour, but is also the result of modifying traditional statistical parameters. Rouvroy and Berns (2013) analyse how the impression of a democratic normativity, which treats everyone equally and which does not impose rules but reflects existing behaviours, is created. The social statistics inherited from Quetelet researches hypotheses with data divided into predefined categories reducible to mathematical means and probabilities, whereas the new systems are developed in simultaneously executed phases, without positing any prior hypotheses or category.

Vast quantities of data are stored automatically, everything is potentially relevant, nothing is filtered, whereby any sort of intentionality is

IC – Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208] E-ISSN: 2173-1071

ruled out in the ledger and their objectivity is guaranteed. Correlations between data are identified automatically and without any predefined hypothesis, eliminating as before any new traces of subjectivity in the analytical process. The analysis does not focus on the subject in question. What is important is not the identity of users, but what they do and when and where they do it. The aim of the profile generated from these data is to avoid a priori any category in order to eliminate any hint of discrimination. As a matter of fact, flesh-and-blood individuals are isolated or detached from their own profiles, of which they are completely unaware more often than not and in which they cannot intervene. And all this despite the fact that predictions are made on their preferences, intentions and propensities that will not directly modify them but the information system with which they interact (Rouvroy & Berns, 2013).

Such expert systems recreate the fiction of a placeless, faceless, bodiless, ahistorical universal knowledge and power under the promise of preventing or eradicating 'deviant' behaviour. This is reflected in the notion of 'machine learning' or 'automated learning', a branch of AI that suggests that systems per se can identify patterns in data and make autonomous decisions, with little or no human intervention, as a prior step to constructing and automating analytical models. Rouvroy and Berns (2013, p. 10) also resort to the notion of 'algorithmic governance' to refer to the normative rationality that predisposes and enables these systems through 'the automated collection, aggregation and analysis of big data so as to model, anticipate and pre-emptively affect possible behaviours'.

Unlike democratic legal normativity, algorithmic governance is not performed publically or discursively before taking any action on a specific behaviour. With the assurance of total objectivity and with action based on anticipating behaviours and rationally assessing risks and opportunities, any anomaly would be assimilated and corrected beforehand. Thus, algorithmic governance deploys a dehumanised horizon of dystopic innovation in which the state would be a conglomerate of corporate expert systems.

This horizon would reduce technological sovereignty to issues associated with the still vague notion of 'software governance'. Nowadays, many things that we use on a daily basis depend on computer apps to function properly. The growing automation of physical objects and processes using big data requires the development, maintenance, cleaning and updating of

E-ISSN: 2173-1071 IC – Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208]

different apps. The simile employed by Shuttleworth and Moglen (2018, p. 1) when suggesting that the methods of '"software governance," are to 21st-century technology what materials science and quality assurance practices were to 20th-century industrial activity', is very telling. Although, as the same authors note, 'They are now a crucial "hidden input" to industry's ability to make, and government's ability to regulate, everything we use' (p. 1).

However, we are not interested in discussing technological sovereignty, 'software governance' or the 'datification' of physical objects and processes emerging from the new algorithmic governance paradigm. Rather, our intention is to describe the reactions of data activism to the automation of democratic bodies and procedures for decision-making and conflict resolution that would guarantee the planned obsolescence of the citizenry.

3. Proactive and reactive data activism

Milán and Gutiérrez (2015, p. 13) distinguish between two main types of data activism, either to exploit available data or to hinder its mass collection, i.e. proactive and reactive data activism. 'Proactive data activism' involves individuals and organisations of civil society that leverage open data and networks to promote social change and to broaden participation in decision-making and conflict resolution processes using socially distributed information systems that they themselves have designed (Gutiérrez, 2018). The geolocalised information of Humanitarian OpenStreetMap, the radiation levels measured by Safecast in the wake of the nuclear disaster in Fukushima (Brown, Franken, Bonner, Dolezal, & Moross, J., 2016), the revision of hundreds of thousands of DNA kits relating to rape cases in the United States thanks to 'Ending the Backlog' (O'Connor, 2003) and the Open Spending project aimed at the disclosure of the most detailed information on government spending ever published, are just a few examples of proactive data activism. Here, our vision of proactive activism includes the work of Ciencia Forense Ciudadana and Data Cívica in Mexico during the war on drugs over the past few years and the initiatives for the direct participation of the citizenry in the decision-making bodies of parliamentary democracies through information systems such as LiquidFeedback, Democracia 4.0 and DemocracyOS.

IC – Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208] E-ISSN: 2173-1071

'Reactive data activism' ensures greater privacy and control in an attempt to prevent the dataveillance inherent to algorithmic governance. Open software alternatives to proprietary algorithms have led to the availability of the source code of operating systems and apps that respect people's privacy. This has favoured the development of free access services and apps, including the 'autonomous servers' of Espora in Mexico, Sindominio in Spain and Austitici/Inventati in Italy, the search engine Duckduckgo, social networking sites, forums and instant messaging services like Diaspora*, GNU, Telegram, Telekommunisten, Riseup, Freenet and Lorea, to name but a few. To these examples of reactive data activism relating to the federated Web, which are decentralised and interoperable (GNU, 2012; Cabello, Franco, & Haché, 2012), should be added encrypted and anonymity systems based on the blockchain and the Onion Router (hereinafter TOR) that probe the depths of the deep and dark web, generating a new P2P network architecture heavily protected against external interference with open and/or free encryption algorithms (Mattila, 2016). These socially distributed information systems based on a strong encryption pose different challenges for algorithmic governance, which we will now analyse below using Silk Road, Bitnation and Democracy Earth Foundation as examples.

4. Criminalisation and reactive data activism: Silk Road

Silk Road was an online platform for selling illegal drugs, launched in February 2011. Its offerings included marihuana, hash, hallucinogenic mushrooms, LSD, ecstasy, DMT and mescaline. It used the anonymity network TOR to encrypt all the traffic to and from its website, for which reason, according to its administrators, it was impossible to know 'who you are or who runs Silk Road. For money, we use Bitcoin, an anonymous digital currency' (cited in Ladegaard, 2017, p. 1).

Silk Road was not the first online black market for drugs (Power, 2013), but was indeed the first to operate with cryptocurrencies on the dark web, employing sophisticated encryption mechanisms to protect the datafiow from external surveillance (Van Hout & Bingham, 2014). Some platforms even

E-ISSN: 2173-1071 IC – Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208]

offered opium and cocaine under the 'organic' and 'fair trade' labels, while even going so far as to claim that the drugs came from 'a conflict-free zone' (Martin, 2014).

The encryption of users and transactions prevented police intervention, thus facilitating trade between clients and vendors whose level of mutual trust was exclusively measured by a reputation system based on public comments and assessments, like those of eBay or Amazon. Clients and vendors were supposed to have faith in the design of a technical system that only some are capable of fully understanding (Ladegaard, 2017).

A few months after being launched, the designers of Silk Road gave an interview in which their claimed, 'The state is the primary source of violence, oppression, theft and all forms of coercion' (Chen, 2011). Later on, the journalist Greenberg (2013) compiled and published further quotes in which a radical liberalism was reaffirmed. This doctrine went hand in glove with the establishment of an ethic that banned users from offering anything whose purpose was to injure or to cheat (Gayathri, 2011), in such a manner that the site became a political statement in favour of the decriminalisation of drugs. In 2013, the FBI prosecuted R. W. Ulbricht as the sole person behind the pseudonym under which the owners of Silk Road operated: 'Dread Pirate Roberts'. Ulbricht was sentenced to life imprisonment with no right of appeal, but cryptomarkets for prohibited substances have continued to proliferate since his prosecution.

In light of the failure of punitive measures, different studies suggest that cryptomarkets reduce the risks that drug trafficking on the streets involves, primarily territorial conflicts between dealers and the pressure exerted by law enforcement agencies, which has reached unprecedented levels in the 'war on drugs' in the United States, Colombia and Mexico (Martin, 2014; Aldridge & Décary-Hétu, 2014; Buxton & Bingham, 2015). These studies have converted Silk Road into an embarrassing example for reactive data activism that evades dataveillance and establishes its own mechanisms for decision-making and conflict resolution, in which neither policies nor official institutions are recognised, but there is trust in the good management of algorithms and the invisible hand of the free market.

The discourses of administrators and users show how part of the citizenry on the streets and on networks perceive the flaws, lacunae and

IC – Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208] E-ISSN: 2173-1071

inconsistencies of the hegemonic governance models as a new exercise of authoritarianism, to which they react by participating in encrypted social networking sites, a topic that we will address further on.

5. Re/inventions of law enforcement agencies and proactive data activism: Ciencia Forense Ciudadana and Data Cívica

Over the past few years, public policies as regards the production, trafficking and consumption of drugs have focused on the war on drugs. In the case of Mexico, the ex-president Felipe Calderón launched, just a few days after being sworn into office, a campaign against organised crime, with the support of the country's armed forces. This initiative, totally lacking in strategy, as Aristegui (2012) observes, resulted in tens of thousands of casualties and thousands of missing or displaced persons. According to official figures, during the Calderón government the number of missing persons jumped to 1,000 per year. For their part, civic organisations estimate that there are between 30,000 and 50,000 missing persons after a decade of the 'war on drugs' (*El País*, undated).

Owing to the inadequate official response to this serious humanitarian crisis, 'a forensic and DNA database, created, managed and used by the relatives of missing persons' (Ciencia Forense Ciudadana, 2014) was launched, in collaboration with the researchers involved in the Citizen Led Forensics project. Cienciaforenseciudadana.org allows families to donate their DNA to the Citizen National Registry of Missing Persons[1], so as to permit the government and civic organisations to contrast the human remains discovered and to identify them.

> Ciencia Forense Ciudadana's most important technology is governance (not only computers, their systems and DNA analysis are technologies), involving the participation of the relatives of missing persons incorporated in a forum

1 In Spanish, Registro Nacional Ciudadano de Personas Desaparecidas.

E-ISSN: 2173-1071 IC – Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208]

> of ethical and technical regulation, which also guides the project's strategic vision' (Ciencia Forense Ciudadana, undated, original emphasis).

The official data obtained from the complaints lodged with the National Registry of Missing Persons[2] (RNPED), managed by the Mexican state, neither served to identify the remains unearthed in 1,075 clandestine mass graves located between 2007 and 2016 (González Núñez & Chávez Vargas, 2017), nor offered an updated or reliable database.

In 2017, Data Cívica published the official figures in an updated and evidenced-based database, with the full names of thousands of missing persons (Reza, 2017).

> In our country, the names of missing persons are not made public. No one knows who they are, what they are like or their stories. We know no more than the number of people who are not here.
> [...] They disappear from the registry without trace, without anyone knowing whether they were removed from the database because they were found alive or because they were found dead. They have disappeared twice.
> This project seeks to give names and a face to the missing persons, so that they can recount their stories. To put a name to the missing people in the RNPED also signifies the chance to demand justice and the truth (Data Cívica, 2017).

A few days after the publication of Personasdesaparecidas.org.mx and following a long wait and much heated debate, the General Law on the Forced Disappearance of Persons and Missing Persons[3] was passed, a piece of legislation that envisages the mandatory publication of the names

2 In Spanish, Registro Nacional de Personas Extraviadas o Desaparecidas.

3 In Spanish, Ley General de Desaparición Forzada de Personas y de Desaparición.

IC – Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208] E-ISSN: 2173-1071

of missing persons in official databases. However, it neither had specific mechanisms for its enforcement nor a budget to fund its activities (Ge, 2017).

The next government of the ex-president Enrique Peña Nieto was accused of using cyberespionage against activists, journalists and human rights activists supporting civic initiatives like those mentioned above (Ahmed & Perlroth, 2017). In the wake of the Pegasus scandal, called after an app originally designed to monitor terrorists and drug traffickers (Reina, 2017), many of the organisations abandoned in protest the Open Government Partnership (OGP), dedicated to enhancing civil big data applications and subscribed and backed by the Mexican state as a founding member (Art. 19, 2017).

6. Beyond the ballot box: from liquid feedback to Bitnation

The aforementioned examples of reactive and proactive data activism encourage us to reconsider official governance models aimed at conflict resolution. Silk Road substituted public policies with a socially distributed and strongly encrypted information system that operated outside the rule of law. Ciencia Forense Ciudadana and Data Cívica have both demonstrated how a sector of civil society has taken responsibility for the victims, assuming the role of official agencies, with their techniques and procedures, tasked, as if it were a police investigation, with the process of criminalisation. Data activism's actual contribution to decision-making remains to be seen.

The Liquidfeedback.org app was created on the margins of any specific political party by the Public Software Group in 2009, as a viable software solution for helping any organisation to make decisions. (Mendoza, 2015). This app is currently being used as an additional communication channel between citizens and their administrations (Behrens, Kistner, Nitsche, & Swierczek, 2014). The Pirate Party Germany was the first to adopt it.

In Spain, Democracia Real Ya, belonging to the 15-M movement, launched Democracia 4.0. This initiative consisted in allowing the citizenry to vote online on all the laws tabled in the Lower House, with a digital certificate issued by the Spanish Congress (Bocanegra, 2011).

E-ISSN: 2173-1071 IC – Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208]

> Our deputies represent popular sovereignty, but national sovereignty in vested in the Spanish people (Art. 1.2 Spanish Constitution).
> As citizens, we want to participate directly in making the decisions that affect us, now that we know that this is possible from home, thanks to the Internet. [...]
> Therefore, this does not involve dispensing with the Congress, deputies, parties or elections. What is being proposed is a combination of both systems of political participation, for we believe that the material and legal conditions are already in place. For which reason, the moment has come to make use of our quota of sovereignty, to decide on our future whenever we want (Democracia 4.0, 2011).

In Argentina, Partidodelared.org uses a free software tool designed in-house, called 'DemocracyOS' (democracyos.org) for 'Democracy on the Web'. 'We are a civic organisation formed by activists, programmers and social scientists who seek to open up the public institutions and decision-making processes' (Democracia en Red, 2014). Siri (2016) states that the Net Party acts like 'a Trojan horse to penetrate the heart of the nation state', thus illustrating the reactive responses to the dual criminalisation of algorithmic control and official techniques, agencies and procedures for decision-making, which hitherto have formed part of the traditional exercise of citizenship.

The horse has replaced the soldiers willing to die in battle with a Silicon Valley funded project developed between 2015 and 2016. Democracy Earth Foundation is inspired by an authoritarian interpretation of hegemonic governance techniques and procedures. According to its creators, 'In this world freedom is an illusion: our bodies belong to governments, our minds to corporations. [...] As this scenario unfolds, encryption plays a role of growing significance to protect the human rights of digital citizens as it can help them break apart from the cloud versus land trap' (Democracy Earth Foundation, 2018, p. 5).

These examples of information systems linked to the notion of 'liquid democracy' or 'delegative democracy' that have appeared in different countries are characterised by facilitating citizen participation in public decision-making

IC – Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208] E-ISSN: 2173-1071

bodies through delegates, revocable at any moment, who (ideally) represent and defend decisions previously voted on online (Behrens, 2017). But the crisis of democratic institutions has added a new twist to software development, like the decentralised governance platform designed for any type of organisation, developed by the Democracy Earth Foundation. To the creation of cryptocoins like Bitcoin, without central banks, this open source software, called 'Sovereign', adds 'an incorruptible voting system' to protect the personal and transnational sovereignty of its members by means of encryption (Siri, 2016). According to its slogan, the ultimate objective is to dismantle the old state by implementing an algorithmic governance without frontiers for 'anyone, anywhere'.

Susanne Tarkowski Tempelhof, CEO and founder of Bitnation–'The Internet of Sovereignty'–has announced the first Decentralized Borderless Voluntary Nation (DBVN), which belongs to the company Bitnation Americas Ltd., based in Belize:

> Bitnation started in July 2014 and hosted the world's first blockchain marriage, birth certificate, refugee emergency ID, World Citizenship, DBVN Constitution and more. The website proof-of-concept, including the blockchain ID and Public Notary, is used by tens of thousands of Bitnation Citizens and Embassies around the world (Bitnation, 2014).

Bitnation allows for creating states to the taste of consumers, designing forms of consensus outside the legal system and issuing one's own coins without any inference from central banks.

Initiatives are based on the possibilities offered by Bitcoin technology and the public ledger of transactions between peers, called 'blockchain'.[4] The transactions made through network nodes using open source cryptographic

4 Blockchain is implemented in all types of educational (Odem, Moodle Open Badges Plugin), health (Etheal), work (CoinLancer), gaming (FairWin, EtherSprots, Tap Project), commercial (Choon, Rentberry), virtual reality (Decentraland, Vibe) and security (Defense Distributed) systems, to name but a few. Companies like Microsoft and Coca-Cola have also become involved in innovation currents revolving around the blockchain (Williams, 2018). For its part, the European Union launched its Blockchain Observatory and Forum at the beginning of 2018 (European Commission, 2018).

E-ISSN: 2173-1071 IC – Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208]

algorithms are recorded and verified without human intervention (proof-of-work), central authority, control point or third-person supervision. In this respect, Atzori (2015, p. 2) indicates that the blockchain system, in addition to being tamper-proof, 'makes human intervention or controlling authority unnecessary'.

Other examples of decentralised algorithmic governance based on the blockchain can be found in decentralised autonomous organisations (DAOs) and decentralised autonomous corporations (DACs) (Buterin, 2014). Both offer individuals and groups the opportunity to redesign their interactions with politics, business and society in general, in an apparently disintermediated, large-scale process based on automated transactions that claim to be incorruptible thanks to encryption.

7. Conclusions

The socially distributed information systems of data activism offer alternative governance models to the hegemonic techniques and procedures of algorithmic governance. The reactive models operate by exerting tight control over the data produced, distributed and used on a social network through their strong encryption. This encryption supposedly facilitates the necessary autonomy for new forms of consensus building by means of transparent algorithms designed with free or open source software available online. The proactive initiatives use open data, assuming the process of criminalisation hitherto the monopoly of the state, activating, supplementing and questioning official conflict resolution mechanisms, without considering their substitution by decentralised governance platforms. The models seeking delegative systems based on apps like Liquid Feedback offer solutions that would supplement and improve the official decision-making bodies inherent to representative democracies. In all cases, it is possible to observe the empowerment of active groups emerging from civil society that explore forms of restoring citizenship and the common good and which reveal the huge flaws in the measures implemented by governments and companies to tackle current governance problems.

Versus the trend towards a generalised behaviourism on the streets and on networks, proactive data activism experiments with situated historical

IC – Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208] E-ISSN: 2173-1071

and geographical information systems to highlight the current asymmetries between the state, the market and the citizenry. These open and participatory information systems give priority to the citizenry in an attempt to revert the dual tendency towards social automation and criminalisation. It is not a sort of statist nostalgia. They are stateless institutional forms, lack official recognition and are not formally integrated into public decision-making or conflict resolution mechanisms. In these movements there is no nostalgia, but a reformulation of the public sphere by means of algorithms and open data that are not without their problems.

In line with Lea (2002), not only algorithmic governance but also data activism would be the result of an anti-statist, liberal and self-responsible civil society, in which ICTs would serve to enhance individual capacities and behaviours, plus emerging forms of organisation outside the public sphere. In other words, re-establishing the social relations of governance by decentralising the exercise of citizenship would not on its own resolve the existing asymmetries. The definition of living together would be left in the hands of a few citizens conditioned, moreover, by external factors outside their control, such as the existing funding sources and the absence or presence of institutional recognition. Nor do the systems of direct participation in governmental decisions guarantee on their own that participation will be on equal terms and can even reproduce old asymmetries.[5] They are not isolated initiatives but movements inserted in broader changes and conflicts. The official trend towards open data and open government can meet the demands of a computerised citizenry aware of the new surveillance and control mechanisms and the voracity of proprietary expert systems designed for companies always requiring more and more data to capitalise on the crisis of the public sphere.

Dataveillance, along with the fragmentation of territorial control and the resurgence of political and social frontiers, has justifiably fuelled the trend towards reactive systems of decentralised algorithmic governance that simulate new institutional forms. These systems seek in anonymity

5 For a description of the crowdsourced drafting of the Constitution of Mexico City, see http://congress.crowd.law/case-constitución-cdmx.html, and GovLab's catalogue of other 'crowdlaw' initiatives: https://catalog.crowd.law/

E-ISSN: 2173-1071 IC – Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208]

and encryption alternatives to the traditional functioning of public/private institutions. However, they can run the risk of reproducing the problems of technological solutionism intrinsic to 'preventive police action' apps. Others risks inherent to these governance models have been noted by Golumbia (2017, p. 109), when recalling that one of the conditions for their existence largely involves an imaginary state of perpetual war (see Assange, 2006, 2012), 'not only involving state and pseudo state, like those that are clearly occurring today, but also all types of non-state actors deploying all types of digital weapons—a category whose real limits are still to be discovered—and, by and large, granting "victory" to whoever manages to accumulate the greatest power, the most solid defence and the strongest army' (Sastre, 2019, in press).

If the Internet becomes a battlefield, the promise of emancipation through the decentralisation and horizontality of this type of reactive activism may share the conservative prospects of those policies criminalising the social sphere. As a result, the public bodies tasked with decision-making and conflict resolution underpinning the exercise of citizenship (or what is left of it) would be substituted by algorithms designed to assess the adequate behavioural limits of each individual and each group inside information systems that very few are capable of understanding or recoding. Despite being decentralised, free and open, these systems promise to offer the ultimate solution to the crisis of present-day democracies by recreating the fiction of a placeless, faceless, bodiless, ahistorical, universal knowledge and power, unblemished by subjective issues, which would make dissent impossible. Any anomaly could be assimilated and immediately corrected, and any political dilemma immediately erased to establish, instead, antagonism as a generalised way of life (Mouffe interviewed by M. López San Miguel, 2010).

8. Bibliography

——— Ahmed, A., & Perlroth, N. (2017, June 19). 'Somos los nuevos enemigos del Estado': el espionaje a activistas y periodistas en México. *The New York Times*, Retrieved from https://www.nytimes.com/es/2017/06/19/mexico-pegasus-nso-group-espionaje/?ref=nyt-es-LA

IC – Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208] E-ISSN: 2173-1071

——— Aldridge, J., & Décary-Hétu, D. (2014, May 13). Not an 'eBay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation. *SSRN*. DOI: 10.2139/ssrn.2436643

——— Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016, May 23). Machine Bias. *ProPublica*, Retrieved from https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

——— Aristegui, C. (2012, November 29). Lo blanco y lo negro del sexenio de Felipe Calderón. *Aristegui Noticias*, Retrieved from https://aristeguinoticias.com/2911/mexico/lo-blanco-y-lo-negro-del-sexenio-de-felipe-calderon/

——— Artículo 19 (2017, May 23). Por espionaje sociedad civil concluye participación en la Alianza para el Gobierno Abierto, Retrieved from https://articulo19.org/por-espionaje-sociedad-civil-concluye-participacion-en-el-secretariado-tecnico-tripartita-de-la-aga/

——— Assange, J. (2006). Conspiracy as Governance, Retrieved from https://web.archive.org/web/20070129125831/http://iq.org/conspiracies.pdf

---- (2012). Introduction: A Call To Cryptographic Arms. In J. Assange (Ed.) (with J. Appelbaum, A. Müller-Maguhn, & J. Zimmermann). *Cypherpunks. Freedom and the Future of the Internet*. New York: OR Books.

——— Atzori, M. (2015). Blockchain Technology and Decentralized Governance: Is the State Still Necessary? *SSRN*. DOI: 10.2139/ssrn.2709713

——— Behrens, J. (2017). The origins of liquid democracy. *The Liquid Democracy Journal, 5*, Retrieved from http://www.liquid-democracy-journal.org/issue/5/The_Liquid_Democracy_Journal-Issue005-02-The_Origins_of_Liquid_Democracy.html

——— Behrens, J., Kistner, A., Nitsche, A., & Swierczek, B. (2014). *The principles of Liquid Feedback*. Berlin: Interaktive Demokratie e. V.

——— Bitnation (2014). *Bitnation*. Retrieved from https://tse.bitnation.co/

——— Bocanegra, R. (2011, October 26). DRY propone que los ciudadanos puedan votar las leyes por Internet. *Público*, Retrieved from https://www.publico.es/espana/dry-propone-ciudadanos-puedan-votar.html

——— Brown, A., Franken, P., Bonner, S., Dolezal, N., & Moross, J. (2016). Safecast: successful citizen-science for radiation measurement and communication after Fukushima. *Journal of Radiological Protection, 36*(2), S82, Retrieved from http://iopscience.iop.org/article/10.1088/0952-4746/36/2/S82

——— Buterin, V. (2014, May 6). DAOS, DACS, DAS and More: An Incomplete Terminology Guide. Ethereum Blog, Retrieved from: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

——— Buxton, J., & Bingham, T. (2015). *The Rise and Challenge of Dark Net Drug Markets*. Policy Brief 7. Swansea University: Global Drug Policy Observatory, Retrieved from https://www.swansea.ac.uk/media/The-Rise-and-Challenge-of-Dark-Net-Drug-Markets.pdf

——— Cabello, F., Franco, M. G., & Haché, A. (2012). Hacia una web social libre y federada: el caso de Lorea. *Teknokultura. Revista de Cultura Digital y Movimientos Sociales*, *9*(1), 19-43.

——— Chen, A. (2011). The Underground Website Where You Can Buy Any Drug Imaginable. *Gawker*, Retrieved from https://web.archive.org/web/20110613040631/http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable

——— Ciencia Forense Ciudadana (2014, September 13). Proyecto Ciencia Forense Ciudadana [video archive]. *Ciencia Forense Ciudadana*, Retrieved from https://www.youtube.com/watch?v=vQGR2A7eKD0

——— Ciencia Forense Ciudadana (n/d). ¿Qué puedo esperar de esta tecnología?. Preguntas Frecuentes, Retrieved from http://cienciaforenseciudadana.org/preguntas-frecuentes/

——— Dastin, J. (2018, October 10). Amazon scraps secret AI recruiting tool that showed bias against women, Reuters, Retrieved from https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G

——— Data Cívica (2017). ¿Por qué lo hicimos? *Personas desaparecidas*, Retrieved from http://personasdesaparecidas.mx/semblanza#why

E-ISSN: 2173-1071 IC – Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208]

IC – Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208] E-ISSN: 2173-1071

——— De la Cueva, J. (2019, in press). La configuración de la tecnología como cuestión política. *Teknokultura. Revista de Cultura Digital y Movimientos Sociales*, *17*(1).

——— Democracia 4.0 (2011). Breve explicación Democracia 4.0, Retrieved from https://web.archive.org/web/20141225093518/http://demo4punto0.net/es/home

——— Democracia en Red (2014). ¿Quiénes somos? *Democracia en Red*, Retrieved from https://democraciaenred.org/

——— Democracy Earth Foundation (2018). *The Social Smart Contract. An Open Source White Paper*, Retrieved from https://github.com/DemocracyEarth/paper/blob/master/README.mediawiki

——— Dick, P. K. (2002 [1956]). *The Minority Report*. New York: Pantheon Books.

——— Europa Press (2018, November 22). Protección de Datos insiste en que es ilegal hacer perfiles ideológicos y estará vigilante a lo que hacen los partidos, Retrieved from https://www.europapress.es/sociedad/noticia-proteccion-datos-insiste-ilegal-hacer-perfiles-ideologicos-estara-vigilante-hacen-partidos-20181122131122.html

——— European Commission (2018, February 1). European Commission Launches the EU Blockchain Observatory and Forum, Retrieved from http://europa.eu/rapid/press-release_IP-18-521_en.htm

——— Gayathri, A. (2011, November 6). From marijuana to LSD, now illegal drugs delivered on your doorstep. *International Business Times*, Retrieved from http://www.ibtimes.com/marijuana-lsd-now-illegal-drugs-delivered-your-doorstep-290021

——— Ge, M. (2017, December 5). Cómo una base de datos en México se adelantó al gobierno para buscar desaparecidos. *School of Data Blog*, Retrieved from https://es.schoolofdata.org/2017/12/05/COMO-UNA-BASE-DE-DATOS-EN-MEXICO-SE-ADELANTO-AL-GOBIERNO-PARA-BUSCAR-DESAPARECIDOS/

——— GNU (2012). The GNU consensus Manifesto, Retrieved from https://www.gnu.org/consensus/manifesto.html

——— Golumbia, D. (2017). The Militarization of Language: Cryptographic Politics and the War of All against All. *Boundary 2*, *44*(4), 95-112. DOI: 10.1215/01903659-4206337

——— González Núñez, D., & Chávez Vargas, L. G. (Coords.) (2017). *Violencia y terror. Hallazgo sobre fosas clandestinas en México*. México: Universidad Iberoamericana y Comisión Mexicana de Defensa y Promoción de Derechos Humanos A.C., Retrieved from http://cmdpdh.org/project/violencia-terror-hallazgos-fosas-clandestinas-mexico/

——— Greenberg, A. (2013, April 29). Collected Quotations of the Dread Pirate Roberts, Founder of Underground Drug Site Silk Road and Radical Libertarian. Forbes, Retrieved from https://www.forbes.com/sites/andygreenberg/2013/04/29/collected-quotations-of-the-dread-pirate-roberts-founder-of-the-drug-site-silk-road-and-radical-libertarian/#36340fd81b0c

——— Gutiérrez, M. (2018). Data activism and social change. Hampshire and New York: Palgrave Macmillan.

——— Habermas, J. (1976). Legitimation Crisis. London: Heinemann.

——— Hall, S., Critcher, C., Jefferson, T., Clarke, J., & Roberts, B. (1978). Policing the Crisis: Mugging, the State, and Law and Order. London: Macmillan.

——— López San Miguel, M. (2010, September 5). La democracia consiste en permitir los puntos de vista. Página 12, Retrieved from https://www.pagina12.com.ar/diario/elmundo/4-152631-2010-09-05.html

——— Nadal, H., & De la Cueva, J. (2012). Redefiniendo la isegoría: open data ciudadanos. In A. Cerrillo i Martínez, M. Peguera, I. Peña-López, M. J. Pifarré de Moner, & M. Vilasau Solana (Coords.), *Retos y oportunidades del entretenimiento en línea* (pp. 283-300). Actas del VIII Congreso Internacional, Internet, Derecho y Política. Barcelona: UOC-Huygens Editorial, Retrieved from http://openaccess.uoc.edu/webapps/o2/bitstream/10609/15121/6/IDP_2012.pdf

——— Ladegaard, I. (2017). We Know Where You Are Doing And We Will Catch You. The British Journal of Criminology, 58(2), 414-433. DOI: 10.1093/bjc/

E-ISSN: 2173-1071 IC – Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208]

IC – Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208] E-ISSN: 2173-1071

——— Lea, J. (2002). Crime and Modernity. Continuities in Left Realist Criminology. London: Sage.

——— Martin, J. (2014). Drugs on the Dark Net: How Cryptomarkets are Transforming the Global Trade in Illicit Drugs. Hampshire and New York: Palgrave Macmillan.

——— Mattila, J. (2016). The Blockchain Phenomenon. Research Institute of the Finnish Economy, Retrieved from http://www.brie.berkeley.edu/wp-content/uploads/2015/02/Juri-Mattila-.pdf

——— Mendoza, N. (2015). Liquid Separation: Three Fundamental Dimensions within LiquidFeedback and other Voting Technologies. eJournal of eDemocracy & Open Government, 7(2), 45-58.

——— Milán, S., & Gutiérrez, M. (2015). Medios ciudadanos y big data: la emergencia del activismo de datos. Mediaciones, 11(14), 10-26.

——— Minuto Político (2019, May 22). El Constitucional anula las bases de datos con perfilado ideológico de los ciudadanos. El diario.es, Retrieved from https://www.eldiario.es/politica/MINUTO-POLITICO-campana-arranque-Congreso_13_901989793.html

——— Morozov, E. (2013). The Folly of Technological Solutionism. To Save Everything, Click Here. New York: PublicAffairs.

——— O'Connor, K. L. P. (2003). Eliminating the Rape-Kit Backlog: Bringing Necessary Changes to the Criminal Justice System. UMKC Law Review, 72, 193-214.

——— O'Neil, C. (2016). Weapons of Math Destruction. New York: Crown Publishers.

——— Pasquinelli, M. (2016). The Spike: On the Growth and Form of Pattern Police. In S. Hankey, M. Tuszynski, & A. Franke (Eds.), Nervous Systems (pp. 245-260). Berlin: HKW/ Spector Books.

——— Pishko, J. (2014, August 18). Punished For Being Poor: The Problem With Using Big Data In The Justice System. Pacific Standard, Retrieved from https://psmag.com/news/punished-poor-problem-using-big-data-justice-system-88651

——— Power, M. (2013, April 19). Online highs are old as the net: the first e-commerce was a drugs deal. The Guardian, Retrieved from https://www.theguardian.com/science/2013/apr/19/online-high-net-drugs-deal

——— Rainie, L., & Anderson, J. (2017, February 8). Code-Dependent: Pros and Cons of the Algorithm Age. Pew Research Center, Retrieved from http://www.pewinternet.org/2017/02/08/code-dependent-pros-and-cons-of-the-algorithm-age

——— Reina, E. (2017, June 20). Pegasus, el programa que espía a los periodistas y activistas mexicanos. El País, Retrieved from https://elpais.com/internacional/2017/06/20/mexico/1497920669_881339.html

——— Reza, G. (2017, November 13). Data Cívica descifra nombres de casi 32 mil desaparecidos y evidencia fallas del RNPED. Proceso, Retrieved from https://www.proceso.com.mx/510968/DATA-CIVICA-DESCIFRA-NOMBRES-CASI-32-MIL-DESAPARECIDOS-EVIDENCIA-FALLAS-DEL-RNPED

——— Rosenblat, A., & Stark, L. (2016). Algorithmic Labor and Information Asymmetries: A Case Study of Uber's Drivers. International Journal of Communication, 10(27), Retrieved from https://ssrn.com/abstract=2686227

——— Rouvroy, A., & Berns, T. (2013). Algorithmic governmentality and prospects of emancipation (trad. E. Libbrecht). *Réseaux*, *1*, 163-196, Retrieved from https://www.cairn-int.info/article-E_RES_177_0163--algorithmic-governmentality-and-prospect.htm

——— Selbst, A. D., & Powles, J. (2017). Meaningful Information and the Right to Explanation. *International Data Privacy Law, 7*(4), 233-242, Retrieved from https://ssrn.com/abstract=3039125

——— Sastre Domínguez, P. (2019, in press). Cómo diseñar el crimen perfecto. In R. Hernández (Ed.), Criminología ambiental. Madrid: Editorial Delta.

——— Shuttleworth, M., & Moglen, E. (2018). Automotive Software Governance and Copyleft, Retrieved from https://www.softwarefreedom.org/resources/2018/automotive-software-governance.pdf

——— Siri, S. (2016, March 30). Future of Democracy. TEDx Talks [video archive], Retrieved from https://www.youtube.com/watch?v=yGmGWZCE4h0

E-ISSN: 2173-1071 IC - Revista Científica de Información y Comunicación 16 (2019) [pp. 183-208]

Tutt, A. (2017). An FDA for Algorithms. 69 Admin. L. Rev., 83, Retrieved from https://ssrn.com/abstract=2747994

Van Hout, M. C., & Bingham, T. (2014). Responsible Vendors, Intelligent Consumers: Silk Road, the Online Revolution in Drug Trading. International Journal of Drug Policy, 25, 183–189.

Williams, S. (2018, April 18). The 3 Most Ambitious Blockchain Projects. The Motley Fool, Retrieved from https://www.fool.com/investing/2018/04/18/the-3-most-ambitious-blockchain-projects.aspx