

# Media Development

3/2020

WACC

E x p a n d i n g

Public  
Communication  
Spaces



- +plus Media viability gets a boost
- Data as public good, and the public sector
- Tensions between media censorship and regulation in Jamaica

# Join the World Association for Christian Communication!

WACC is an international organization that promotes communication as a basic human right, essential to people's dignity and community. Rooted in Christian faith, WACC works with all those denied the right to communicate because of status, identity, or gender. It advocates full access to information and communication, and promotes open and diverse media. WACC strengthens networks of communicators to advance peace, understanding and justice.

## MEMBERSHIP OPPORTUNITIES

Membership of WACC provides opportunities to network with people of similar interests and values, to learn about and support WACC's work, and to exchange information about global and local questions of communication rights and the democratization of the media.

WACC Members are linked to a Regional Association for the geographic area in which they are based. They receive regular publications, an annual report, and other materials. Regional Associations also produce newsletters. In addition, members are invited to participate in regional and global activities such as seminars, workshops, and webinars.

Full details can be found on WACC's web site:

[www.waccglobal.org](http://www.waccglobal.org)

## CURRENT MEMBERSHIP RATES

North America	40 USD (Individual)
	120 USD (Institutional)
Rest of the World	35 USD (Individual)
	110 USD (Institutional)
Student Rate	20 USD

*Media Development* is published quarterly by the World Association for Christian Communication  
308 Main Street  
Toronto, Ontario M4C 4X7, Canada.  
Tel: 416-691-1999  
[www.waccglobal.org](http://www.waccglobal.org)

Editor: Philip Lee

## Editorial Consultants

Embert Charles (*Chairperson of the Msgr. Patrick Anthony Folk Research Centre (FRC) of Saint Lucia*)  
Clifford G. Christians (*University of Illinois, Urbana-Champaign, USA*).  
Margaret Gallagher (*Communications Consultant, United Kingdom*).  
Cees J. Hamelink (*University of Amsterdam, Netherlands*).  
Patricia A. Made (*Journalist and Media Trainer, Harare, Zimbabwe*).  
Robert W. McChesney (*University of Illinois, Urbana-Champaign, USA*).  
Samuel W. Meshack (*Hindustan Bible Institute & College, Chennai, India*)  
Francis Nyamnjoh (*CODESRIA, Dakar, Senegal*).  
Rossana Reguillo (*University of Guadalajara, Mexico*).  
Clemencia Rodriguez (*Temple University, USA*).  
Ubonrat Siriyuvasek (*Chulalongkorn University, Bangkok, Thailand*)  
Pradip Thomas (*University of Queensland, Brisbane, Australia*).

## Subscriptions to *Media Development*

Individuals worldwide US\$40.

Libraries and institutions in North America and Europe US\$75.

Libraries and institutions elsewhere in the world US\$50.

The contents of *Media Development* may be reproduced only with permission. Opinions expressed in the journal are not necessarily those of the Editor or of WACC.

Cover design: Brad Collicott

Published in Canada

ISSN 0143-5558

- |  |  |
|--|--|
| 4 Editorial  | 20 Digital justice manifesto: A call to own our digital future                                   |
| 5 COVID-19 pandemic and biopolitics in Latin America<br>Silvio Waisbord and María Soledad Segura | 25 Manifeste pour une justice numérique : Appel à prendre en main notre avenir numérique         |
| 8 SDGs: The challenge to improve lives after the COVID-19 crisis<br>Alexander Trepelkov          | 31 Manifiesto por la justicia digital: Un llamado para que nuestro futuro digital nos pertenezca |
| 10 Sensibiliser sur le COVID-19 : Un travail complexe<br>Mathilde Kpalla                         | 37 Data as public good, and the public sector<br>Parminder Jeet Singh                            |
| 10 India and COVID-19: A communication failure<br>Vincent Rajkumar                               | 41 Media viability gets a boost<br>Lorenzo Vargas  |
| 12 La pandemia de COVID-19 y la pulsión por la vigilancia estatal<br>J. Carlos Lara              | 44 Tensions between media censorship and regulation in Jamaica<br>Brittany Forsythe              |
| 15 The Girona Manifesto on Linguistic Rights   | 47 IAMCR anti-racism statements  |
| 16 European Charter for Regional or Minority Languages (1998)                                    | 49 On the screen   |
| 17 Charte européenne des langues régionales ou minoritaires (1998)                               |  |
| 17 Promotion and use of multilingualism and universal access to cyberspace (2003)                |  |



WACC is a member of the  
**actalliance**

# EDITORIAL

Mainstream media have produced extraordinary and sustained coverage of the COVID-19 pandemic, focusing on health, care-workers, and government policies, as well as the impact on individuals and communities. The same cannot be said for social media, which have been the source of misinformation and fake news, amplifying rumour and stoking fear.

In times of crisis, information saves lives. Responding to COVID-19, it is vital to get accurate and trustworthy messages to people so that they know what they need to do and where they can get help. For many communities, however, particularly those most marginalized such as Indigenous peoples, refugees, and people living in rural poverty, lack of access to mainstream media and sources of information in their own languages increases vulnerability.

Consequently, during the COVID-19 pandemic, many community media outlets took immediate action to provide up to date and accurate information to listeners and viewers. One example comes from Farm Radio International, (FRI) with its connections to 1,000 radio stations across 41 countries in Africa serving 250 million listeners. Aware of the critical importance of clear, accurate, informative broadcasts about COVID-19, FRI began:

- \* Actively distributing information and resources, including scripts and backgrounders, about how to plan and produce effective COVID-19 radio programming;
- \* Creating or activating spaces, such as WhatsApp groups, to give radio broadcasters a place to learn from each other about best practices in COVID-19 radio programming;
- \* Developing connections between broadcasters and public health authorities in government, multilateral and international organizations and civil society to ensure accurate information

goes out and myths are debunked;

- \* Reminding broadcasters of the steps they can take to stay healthy;
- \* Commending broadcasters and other journalists for being on the front line and continuing to work in these conditions.

Over the next year, many studies are likely to be published reviewing lessons learned and planning for the next pandemic. This issue of *Media Development* merely scratches the surface of the various issues, one of which is the importance of local languages.

## Language matters

Globalisation and cultural homogenisation mean that many of the world's 7,117 different languages are in danger of vanishing. UNESCO has identified 2,500 which, it claims, are at risk of extinction. A language becomes endangered when its users begin to teach and speak a more dominant language to their children.

Endangered languages often have few speakers left and it may be difficult to get information about them. One quarter of the world's languages are spoken by fewer than 1,000 people and if these are not passed down to the next generation, they will be gone forever. In 2010, the Bo language – once spoken on the west central coast of North Andaman and on North Reef Island of the Andaman Islands in India – vanished

## ENDANGERED LANGUAGES

THERE ARE AROUND

**7,000  
LANGUAGES  
IN THE WORLD**

**ENGLISH  
IS THE MOST  
SPOKEN  
LANGUAGE  
WITH AROUND  
1,500  
MILLION  
SPEAKERS**

**400**

**LANGUAGES  
ACCOUNT FOR  
95% OF THE  
WORLD'S  
POPULATION**

**REMAINING  
LANGUAGES  
ARE SPOKEN  
BY ONLY  
5% OF PEOPLE**

**1 LANGUAGE**

**DISAPPEARS  
EVERY 2 WEEKS**



**AROUND 18  
LANGUAGES  
HAVE ONLY ONE  
REMAINING SPEAKER**

when an 85-year-old woman of the Bo tribe died.

The first language used on the Internet was almost certainly English. By the mid 1990s it was estimated that English made up 80% of the content. However, from once dominating the web, English now represents just one among an online linguistic elite. English's relative share of cyberspace has shrunk to around 30%, while French, German, Spanish, and Chinese have all pushed into the top 10 languages online. Today that top 10 makes up 82% of the total content on the Internet.

This technological silencing of other languages becomes all the more significant when it comes to facing humanitarian crises such as those posed by COVID-19 or climate change. Language profoundly affects a user's experience of the Internet and determines interactions on social media. It controls how much – if any – information a user can access on Wikipedia and in Google searches.

On Twitter, although English is still the most common language, an estimated 49% of tweets are in other languages, with Japanese, Spanish, Portuguese, and Indonesian users most active. Behaviour analysis shows Twitter users tend to confine their follows, tweets and retweets to those that speak the same language. Theoretically it's a platform for global conversations, but in reality these interactions are fragmented and often limited by language.

Community media in local languages can overcome some of these barriers and help bring about greater resilience and adaptation. Digital platforms are also language-friendly and can be sources of trustworthy and useful information. However, as the Just Net Coalition (whose "Digital Justice Manifesto" is reprinted in this issue of *Media Development*) points out, "Digital governance must aim at a complete break with the current vertically-integrated global digital models... A new digital model must be shaped that is local-to-global; that supports localness and furthers democratic self-determination, without compromising on the important benefits of the globalness of the digital." ■

# COVID-19 pandemic and biopolitics in Latin America

**Silvio Waisbord and María Soledad Segura**

*Does the COVID-19 pandemic mark the birth of a new form of biopolitics? The Latin American case shows important departures from Europe and the United States, both in the adoption of surveillance technologies and in the types of biopolitical control enacted through them.*

As the first pandemic in the datafied society, the COVID-19 pandemic offers an opportunity to reassess debates about digital communication and governability. At the core of these debates is the interest in understanding particular aspects of digital biopolitics – the ambitious efforts by governments and corporations to maximize knowledge and control of populations for political and economic power, as well as the vulnerability of democratic rights such as privacy and the right to know. In a recent article, [Stefan Ecks \(2020\)](#) concludes "we have never seen biopolitics on such a scale. 2020 is the birth year of radical biopolitics."

Given our longstanding interest in the datafied society in Latin America, we are interested in assessing the applicability in the region of arguments about contemporary biopolitics in Europe and the United States. Even if it is early to draw categorical conclusions given that we are in the middle of the pandemic and its evolution and aftermath are unpredictable, there are indications that the current situation in the region does not match recent conclusions about the es-

calation of biopolitics.

At the time of this writing [June 3, 2020], Latin America has become the [new epicenter](#) of the pandemic with growing number of reported cases of infections and deaths. Various governments in Latin America (Peru, Argentina, Bolivia, Chile, Ecuador, Mexico, Colombia and Brazil) and the Inter-American Development Bank have deployed digital technologies to control the transmission of the virus and to support testing and tracing. They have collaborated with private companies and universities in setting up mobile applications for geolocalizing and contact-tracing possibly infected people. Expectedly, these actions have raised concerns about the negative impact of massive surveillance.

### Technological and institutional obstacles

However, while we recognize the legitimacy of these concerns, the problem in Latin America takes different dimensions than in Europe, North America, and East Asia. For the moment, the governments in the region have significant problems to launch and maintain massive digital surveillance apparatuses. What stands in the way of pandemic-driven biopolitics is not a firm official commitment to protecting personal data or to balancing public health objectives and democratic rights. The obstacles are rather technological and institutional, namely, poor reach and limited effectiveness of digital and mobile technologies as well as deep-seated problems of state performance in terms of governmentality and the provision of health services in the region.

Various factors shape biopolitics: government objectives, adequate bureaucratic systems to manage large-scale operations, accountability and transparency of mechanisms and policies, the reliability of digital platforms, and the current conditions of epidemiological surveillance in each country. None of these aspects in Latin America are comparable to the situation in most countries in the global North.

Most national health systems suffer from chronic and severe deficits in the provision of services and the monitoring of populations. Health

systems traditionally underserved large swaths of the population and have been chronically [underfunded](#) and [unequal](#). Also, they have lacked effective government administrative systems to set up, conduct, and maintain massive monitoring based on health and other personal data. Underreported health data is common; in some countries such as Nicaragua, Peru and Venezuela, health authorities have not bothered even to report basic epidemiological data. Underreporting of cases is widely suspected.

It is hard to imagine that suddenly health systems in combination with other government agencies would be set up well-lubricated apparatuses. Take, for example, the decision by Brazil's President Jair Bolsonaro to terminate the agreement between telecommunications companies and the Ministry of Science, Technology, Innovation and Communication to provide information on mobile phones related to geographic location and mobilization. The decision was driven by Bolsonaro's reckless pandemic policy than by concerns about data protection. His government has had an appalling performance since the beginning of the pandemic and it has flatly dismissed concerns raised by health experts (including his former Ministry of Health Nelson Teich) and the World Health Organization.

Official disinterest in mobilizing digital technologies to control the pandemic pales in comparison to the way that police, military and intelligence services in the region have historically approached communication and information technologies for securitization. Since the early decades of the 20th century until recent military dictatorships and contemporary democracies, governments have developed [surveillance technologies](#) to control populations, often with funding and technical support from foreign countries.

Recently, governments in various countries, including Colombia, Mexico, and Guatemala, have beefed up surveillance technologies to spy on critics including human rights activists, politicians and journalists. Nowhere in the region did national governments show comparable interest in incorporating digital technologies to maxi-



Image courtesy of Datac-tive.

mize biopolitics. The differences are quite telling and show different priorities and approaches to surveillance and population management.

Another difference is that digital technologies do not provide significant results without a high rate of adoption of contact tracing and geo-localization applications via cell phones. Their usefulness to contribute to control the pandemic would be quite limited due to technological limitations, namely, the restricted availability of high-end cell phone equipment with Bluetooth and GPS and the unequal infrastructure of cell coverage in the region. Also, a well-functioning digital system would require relatively updated mobile phones, which is not the case among vast numbers of people, as civil society organization such as [Derechos Digitales](#) and [Fundación Sadosky](#) have observed.

According to 2010 data, between 65% and 85% of households own mobile phones in Latin American countries, except for Cuba and Venezuela where [numbers are lower](#). Although a more recent [survey](#) shows that 89% of Latin Americans have a cell phone and 47% a smartphone are used with prepaid plans. In addition, mobile phone services in many countries, such as Mexico, Argentina, Brazil, Colombia and Venezuela, are [the targets](#) of frequent complaints for poor quality, according to consumer rights protection associations.

Also, current health applications use considerable battery power and memory space, which would reduce people's willingness to use them. That is why Apple and Google, the two largest providers of operating systems for cell phones, joined forces to address this issue. Nonetheless, it is not clear yet whether digital corporations will make certain applications available in older mobile phones which are common in the region.

Finally, application malfunctions during the somewhat chaotic launch of COVID-19 in several countries have discouraged people from using them. Due to poor design, applications had many vulnerabilities. This was the case in Argentina in the province of San Luis, where national identity documents (including the processing code that is an authentication factor and the photo) were leaked, and in Buenos Aires where it is possible to access to the date of birth and address of any citizen.

### Uncertain results prevail

In summary, the pandemic has prompted state-directed plans for monitoring COVID-19 prevalence in partnerships with digital corporations and universities, but their results are uncertain at the moment. It is not clear that they would achieve expected results. The obstacle is not a strong culture of privacy and data protection, but rather, chronic problems in government agencies

to ensure that health systems have ample and quality coverage coupled with weak and uneven commitment to addressing the pandemic.

In countries with serious infrastructure problems and insufficient funding for health services, it would have been surprising if governments had actively promoted data tracking to inform healthcare research and policy and fix intractable problems. Indeed, the spotty record of health systems in the region in responding to dengue, zika, Chagas and other infectious disease [outbreaks](#) in recent years suggests that government negligence and lethargy are not conducive to deploying massive digital-based monitoring and interventions.

Knowing the scope of the disease implies collecting massive amounts of data on populations, improving reporting systems, and deploying state-of-the-art technologies – all tasks that demand the kind of government commitment that has been notoriously lacking in health systems in the region. Biopolitics assumes the willingness of states to know and roll out systems to track and control populations. On health matters, Latin American states have largely lacked the political will as well as human, economic and technical resources to know and act. ■

*Reprinted from [Datactive](#) under the Creative Commons license Attribution-ShareAlike 4.0 International.*

Silvio Waisbord is a professor in the School of Media and Public Affairs at the George Washington University, USA.

María Soledad Segura is the director of the research team Sociedad civil y democratización de la comunicación y la cultura, Universidad Nacional de Córdoba, Argentina.

# SDGs: The challenge to improve lives after the COVID-19 crisis

Alexander Trepelkov

*The Sustainable Development Goals (SDGs), with their universal scope, interlinked nature and focus on leaving no one behind will be more essential than ever during and after this crisis.*

The SDGs encourage investments in critical public goods like minimum levels of social protection and the provision of services like health care, clean water and education which help to build resilience and enhance the mechanisms people have to cope with the immediate and longer-term impact of shocks.

The most recent estimates indicate that some 3 billion people are without basic hand-washing facilities at home and 4 billion people lack any kind of social protection.

The SDGs are a commitment to leave no one behind, and this includes ensuring everyone is able to take measures to reduce their exposure to the disease and have the means to cope and recover.

If anything, the SDGs will become more important in the days and months ahead. The goals and targets set in 2015 are precisely the areas where progress needs to be made to build resilience and guard against future crises and where we will need to work to build back after the immediate tragedy subsides.

Preliminary projections from the UN system indicate that COVID-19 could lead to the first increase in global extreme poverty in over 20 years, since the Asian financial crisis of 1981. It

could push 40 to 60 million people into extreme poverty and could double the incidence of food insecurity in the world.

The challenge for improving people's lives after this crisis will be greater than ever, but the SDGs will help guide the path forward to ease suffering.

### **Do any goals stand out at the moment as most pressing?**

Because the SDGs are all interconnected, interventions can be taken in ways that achieve one goal while also leveraging positive synergies among other goals to have a wider reach. The UN's Department of Economic and Social Affairs (DESA) launched the Global Sustainable Development Report last September and a key message there was that taking advantage of synergies and addressing trade-offs among goals is the only way to achieve the 2030 Agenda.

Strengthening human well-being was identified in the report as an entry point for maximizing progress across the Agenda and there are examples that investing in education in science and technology can help build capacities for responding to pressing challenges like climate change and also like the current pandemic.

The report also emphasizes the need for increasing access to social protection as economies change and people need to cope with disasters, including health related; and the need for increasing support for workers to transition to new types of work when livelihoods are dependent on unsustainable sectors.

All of these are policy arenas that will be at the forefront of decision-makers' attention as countries grapple with responses to COVID-19 and try to build stronger social and economic systems to reduce future vulnerabilities.

### **Are they unrealistic? What about the 2030 deadline in light of the pandemic?**

The science and knowledge needed to achieve the 2030 Agenda is well advanced and from a science perspective, the COVID-19 pandemic may even

encourage greater collaboration and knowledge sharing for the public good.

There are also some surprising trends in areas of the 2030 Agenda where progress has been slow. There is evidence that lockdown policies and the resulting reductions in economic activity have seen CO<sub>2</sub> emissions decline substantially.

The conditions of these declines have been tragic and with loss of human lives and livelihoods. But there are questions now as to whether some of the shifts in human activity in response to COVID-19 government implemented guidelines could open space for dialogue about behaviour changes that can support longer term climate action.

So, we have the evidence needed to take action and possibly the space to make significant policy changes. But to be successful, all stakeholders should be involved in dialogue and inform the decision-making processes.

Two annual events that DESA organizes can provide a model for multi-stakeholder engagement and decision-making: the Science, Technology and Innovation Forum (STI Forum) and the High Level Political Forum on Sustainable Development (HLPF). ■

*Source: Republished with permission from [Inter Press Service \(IPS\)](#).*

Alexander Trepelkov is Officer-in-Charge of the Division for Sustainable Development Goals (SDGs) at the UN's Department of Economic and Social Affairs (DESA).

# Sensibiliser sur le COVID-19 : Un travail complexe

Mathilde Kpalla

*Le Togo, comme la plupart des pays de l'Afrique subsaharienne, est touché par le COVID-19. Pour le moment (mars 2020) pas à une grande échelle. Ainsi le Togo en est à 84 cas confirmés et 6 décès.*

Toutefois, dans la crainte que l'épidémie ne prenne une ampleur dramatique, dans un pays avec un système sanitaire précaire, des dispositions sont prises au jour le jour pour prévenir la maladie. Et une des stratégies est la sensibilisation afin que les populations aient le maximum d'informations qui leur permettent de se protéger de la maladie.

Alors les medias sont mis à contribution, tous les médias, officiels, séculaires, communautaires. La radio, la télévision, la presse écrite, la presse en ligne, tous sont engagés dans cette lutte contre le Coronavirus.

Radio Ephphatha, la Voix du Presbytérien, est une radio confessionnelle appartenant à l'Eglise Evangélique Presbytérienne du Togo. Elle est aussi sur le front dans cette sensibilisation. La tâche n'est pas aisée. En effet, les populations au Togo, ont toujours su transcender leurs problèmes, souffrance et autres au travers de leur foi, par une confiance en un Dieu qui peut tout. Et dans le cas d'espèce, un Dieu qui peut les exempter de la maladie. Du coup pour certains, il n'est pas question de respecter les mesures barrières pour prévenir la maladie, mais prier simplement.

Alors nous essayons d'avoir des programmes qui expliquent aux auditeurs, qu'il faut bien prier mais il faut aussi respecter les consignes de sécurité. Il faut donc montrer la compatibilité entre ces mesures et la Bible. Les Eglises étant fermées, le seul moyen de toucher les fidèles

reste la radio, pour que le refus de certains de ne pas respecter les règles ne mette en péril toute la communauté. Il faut aussi pouvoir toucher le maximum, et surtout les couches vulnérables en intensifiant les programmes en langues locales.

L'autre élément qui est pris en compte dans les programmes est le travail de déconstruction à faire par rapport aux multiples fausses informations qui circulent par Whatsapp et qui déroutent les uns et les autres.

Alors pour y arriver, nous faisons intervenir des pasteurs, de médecins, des psychosociologues. Car au-delà de la maladie elle-même, la psychose reste un sérieux problème auquel les populations font face.

Plus que jamais donc, cette sensibilisation doit continuer pour que tous ait la même compréhension de la situation sanitaire, ce n'est que comme cela que la lutte contre le COVID-19 sera efficace. Car un seul porteur du virus dans un coin reculé suffit pour entraîner une contamination en masse. ■

Kpalla Mathilde. Directrice des Programmes de Radio Ephphatha, la Voix du Presbytérien.

## India and COVID-19: A communication failure

*As India grapples with COVID-19, confused and often disempowering communication has aggravated our present predicament.*

Vincent Rajkumar

The Indian Prime minister's address to the nation managed to turn a state of public health crisis into a state of collective paranoia. For a consummate communicator like him, his address to the nation was a model of how not to com-

municate during a health emergency. The Prime minister chose to give Indians barely a four-hour notice. He did not share facts about the government's level of preparedness, nor did he comfort the public regarding the quality of our doctors and medical researchers. He did not explain what would be permitted in this "curfew-like" lockdown, resulting in a late night raid on markets. Worse, he did not offer any assurance to the most vulnerable people that the government would look after their food and other basic requirements, resulting in an exodus of thousands of poor migrants.

During times of crisis, the government has to over-communicate. It, however, chose to under-communicate. This lopsided communication has caused severe suffering among the poor, especially migrant workers, and has been unsuccessful in the primary objective of enforcing social distancing. Those in charge should realise that poorly communicated or insufficient information directly impacts disease control. It results in stigma, fear and poor health-seeking behaviour, and increases vulnerability. It also causes lopsided reporting, theorising and fake news.

At the height of a national emergency, the system is focused on Public Relations rather than governance. The government should have begun a media engagement strategy, along with a multilingual, information campaign on every aspect of the crisis. The response should have been communicated in painstaking detail to the implementers, the media and the public. Instead the government went into an appeal to the Apex court to restrain the media from reporting or publishing "anything" without ascertaining the factual position from the government.

This plea of the Indian government indicates a democratic deficit in the executive in realising the role of the media during a pandemic and the necessity for a credible information ecosystem. While the apex court upheld the right to free discussion about Covid-19, it also directed the media to refer to and publish the official version of the developments in order to avoid inaccuracies and large-scale panic. Herein lies the

catch. It is a fact that fake news and deliberate misleading of the public happens from the top, and often through people who wield power. The government doesn't seem to realise that India's people are more vulnerable to incorrect information if the government and the media do not give them the right information first.

Within this ample framework of complexity, we are involved in research addressing media impact and its role during the COVID-19 pandemic, in the following subtopics:

- \* Effective health communication for the adoption of sustainable preventive measures and curtailing misinformation;
- \* Public health communication to increase psychological resources and resilience in distinct age groups and socioeconomic conditions;
- \* Effective strategies for helping individuals in dealing with social and physical distancing;
- \* Reduction of stigma, prejudice, discrimination, and inequalities.

As we engage in these aspects, we involve in the relief activities that we undertake at this moment with people of all faiths to look after the basic needs of the migrant workers who are either on roads or in temporary sheds at various places. Passing on information at this stage is a really difficult one but social media helps us in coordinating our efforts and also in our communication. ■

Vincent Rajkumar is Director of the Christian Institute for the Study of Religion and Society, India.

# La pandemia de COVID-19 y la pulsión por la vigilancia estatal

J. Carlos Lara

*Incontables iniciativas estatales y privadas pretenden proveer de soluciones a la expansión del COVID-19, incluso en América Latina. A pesar de los llamados a la cordura y al respeto por los derechos fundamentales, persiste en nuestra región un intento por usar la vigilancia como solución, inclusive para problemas que van más allá de la salud pública. ¿Sobreviviremos al brote de vigilancia?*

Desde hace semanas, hemos visto cómo gobiernos mundiales, incluidos los de América Latina, han comenzado a utilizar información de teléfonos móviles y de aplicaciones para teléfonos móviles con el propósito de controlar la expansión de COVID-19 en sus países, fundamentalmente a través de aplicaciones para smartphones. Aunque muchos de los esfuerzos gubernamentales coinciden en carecer de suficiente legitimación y de resguardos de derechos fundamentales, el pánico aparente se convierte en el caldo de cultivo para medidas inidóneas y abusivas.

En un contexto de emergencia global, el problema que surge no es una cuestión solamente del respeto a los derechos en una situación excepcional, sino también del riesgo que significa mantener esa excepcionalidad para el ejercicio de derechos fundamentales a lo largo del tiempo.

## El poder sanador de los datos personales

Una tradicional expresión de la vigilancia es-

tatal es la relativa al seguimiento de personas en sus movimientos y en sus comunicaciones, con las tecnologías de comunicación (y en particular, las digitales) como vía principal para la observación estatal. En un contexto donde resulta conveniente hacer el seguimiento de personas específicas o de grupos numerosos para trazar rutas de contagio o medir situaciones de riesgo, aparecen estas tecnologías como un mecanismo en apariencia idóneo. Varias medidas estatales reflejan esa intuición.

La proliferación de aplicaciones móviles para la pandemia, especialmente a nivel gubernamental, son una muestra básica de esta pretensión. En el caso de las de nuestra región, tanto el rastreo como la entrega de información para el auto-diagnóstico de síntomas asociados a COVID-19 parecen objetivos de política pública razonables para una crisis de salud. Sin embargo, un examen apenas superficial permite encontrar incontables puntos de duda: cómo se anonimizará y agregará la información para no identificar individuos, quién tiene acceso a la información, cómo será utilizada (y en contraste con qué otros datos), por cuánto tiempo y bajo qué condiciones se almacenará, etcétera. Su utilidad en relación con sus niveles de penetración, en tanto, son todavía un misterio.

Como era de esperarse, una situación de crisis para los gobiernos constituye una enorme oportunidad para quienes quieren vender soluciones. Esto es especialmente notorio en el caso de la tecnología, donde cada vendedor ajusta su oferta para convertirla en solución. Es el caso de NSO Group, compañía de tecnologías para la vigilancia, que comenzó a ofrecer y a probar sus capacidades de vigilancia para hacer el seguimiento de personas contagiadas y de las que por estar en contacto con ellas fueran susceptibles al contagio, a partir del cruce de información de dispositivos y de redes de comunicación. Es decir, convirtiendo en una situación deseable parte de la tecnología que ha sido usada incluso en nuestra región, para espiar a periodistas y activistas en México. Además de la falta de credibilidad de oferentes así, ¿cómo puede garantizarse que

la información no se usará con otros fines ni más allá de la emergencia actual?

Fue en la Ciudad de México donde el anuncio de implementación de georreferenciación de telefonía móvil para monitorear movimiento y contacto y controlar el aislamiento social. Como señala R3D, otras autoridades estatales dirigen solicitudes de información a las empresas de telecomunicaciones, sin condición alguna de transparencia para medir su cumplimiento de los estándares de derechos humanos y de la legislación nacional.

En sentido similar, hemos hecho mención al caso de Ecuador, donde se ha dispuesto el uso de “plataformas satelitales y de telefonía móvil” para el control de movimiento de la población bajo aislamiento y cuarentena. A pesar de la pre-

## **Recent issues of Media Development**

2/2020 Traditional Knowledge and Climate Change: Bridging the Gap

1/2020 Realising Gender Equality: Progress and Problems

4/2019 Communication Pirates of the Caribbean

3/2019 MacBride+40: What Next for Media Democracy?

2/2019 Wanted: Sustainable Development Goal 18

1/2019 Brave New Digital World

*Media Development* is provided free to WACC Individual and Institutional Members and is also available by subscription.

For more information visit the WACC website:

[www.waccglobal.org](http://www.waccglobal.org)

ocupación de la sociedad civil a nivel regional y global por la necesidad de resguardos explícitos, en un país donde todavía no existe siquiera una ley de protección de datos personales, la medida de aparente carácter excepcional parece haber seguido su curso, aun cuando Ecuador sigue siendo uno de los países más afectados en número total y proporcional de casos fatales en la región.

En el caso de Brasil, aun cuando por su carácter federal han sido varios los estados que han tomado medidas de prevención y de seguimiento, incluyendo mediante órdenes de aislamiento y del recurso a datos de empresas de telecomunicaciones, la ausencia de órdenes a nivel nacional ha sido patente, y ha estado marcada por el liderazgo temerario del actual presidente de la unión. Una situación particularmente preocupante en atención a que Brasil mantiene el número más alto de contagios en la región. A la anticipada postergación de la entrada en vigor de la Ley General de Datos Personales, se sumó otra preocupación: hace semanas, se hizo público el acuerdo entre empresas de telecomunicaciones y el Ministerio de Ciencia, Tecnología, Innovación y Comunicación, para facilitar información sobre teléfonos móviles relativas a ubicación geográfica y movilización. Días después, tal acuerdo fue rescindido por el presidente Bolsonaro, no necesariamente por preocupaciones sobre los datos personales, como por su actitud temeraria frente a la pandemia. No obstante, los estados conservan capacidad –y más importante, voluntad– para acordar tales usos, como ocurre con los populoso San Pablo y Río de Janeiro.

Otras medidas son aun menos sofisticadas, y pueden igualmente derivar en recolección de información personal. Así, por ejemplo, aplicaciones como el número de WhatsApp dispuesto por el gobierno argentino para recibir consultas facilitando el autoexamen, permiten a la vez identificar números telefónicos y por esa vía a las personas que buscan esa información.

Sea que se trate de georeferenciación mediante antenas de telefonía celular, mediante GPS, mediante señal de WiFi o mediante la entrega voluntaria de información del lugar de cuaren-

tena, resulta al menos cuestionable su real efectividad, en la medida en que no es tanto el rastreo como lo son el aislamiento y las medidas de contención las medidas mejor convocadas a la prevención, como hemos señalado. Es necesaria en cualquier caso una mayor precisión de la información generada –junto a todos los resguardos latamente reiterados– para que ella tenga real capacidad preventiva e informativa en torno a posibles focos de contagio. De lo contrario, la información agregada y anonimizada es la que mejor serviría a la toma de decisiones, también en tal caso bajo resguardos serios, y sin por ello ser por sí sola información suficiente.

## Síntomas de un problema mayor: el control social

Al creciente listado de corona-apps presentes en América Latina se ha sumado más recientemente la anunciada aplicación CoronApp del gobierno de Chile. Como otras, permite el autoexamen y la entrega de información, y permite asimismo registrar el lugar de cuarentena, aun cuando no entrega información de proximidad con personas infectadas. Pero agrega una funcionalidad que varios estados de la región han convertido también en una prioridad: la vigilancia mutua y el control social, más allá de los contagios.

En el caso de la CoronApp chilena, existe una funcionalidad específica para “informar y/o denunciar conductas o eventos de alto riesgo”, esto es, para acusar a la autoridad (en teoría, el Ministerio de Salud) que se están presenciando eventos de aglomeración de personas, incumplimiento de las cuarentenas obligatorias, o existencia de filas para servicios. Es fácil adivinar que esta función puede servir para actos de revancha o enemistad social, quizás empeorando la distancia que ya se ha vuelto costumbre entre personas que comparten áreas con alta densidad demográfica, invocando tal vez innecesariamente a autoridades ya sobreexigidas por una crisis sanitaria global.

Tampoco se trata de una medida de control única. Así, Río de Janeiro controla aglomeraciones mediante denuncias telefónicas y

mediante WhatsApp, además de servirse de información de telefonía móvil, y desde esta semana del uso de drones para seguir movimientos de personas y dirigirse a ellas por altoparlante. En tanto, en sentido similar, Argentina ha dispuesto diversos mecanismos de denuncia, incluida una línea telefónica para denunciar infracciones del aislamiento social. Así, la irresponsabilidad de las personas que insisten en romper situaciones de cuarentena pasa a ser una preocupación adicional de quienes sí la respetan, una fuente de desconfianza social, y una motivación para el control mutuo.

Otro nivel de control que toma como excusa a la pandemia es el realizado por el estado argentino, en el denominado ciberpatrullaje, consistente en la revisión de la discusión en redes sociales “para la prevención de delitos promovidos según el ‘humor social’”. Si bien se trata a menudo de discusiones al alcance del público, esta acción de vigilancia estatal, de no ser transparente y sujeta a protocolos de ejercicio y de control, puede además de ser arbitraria impactar negativamente en las personas, incitando a la autocensura. En ausencia de resguardos sobre su procedencia y su supervisión, puede ser también una forma de vigilancia masiva contraria a los derechos humanos.

## Contra los brotes de vigilancia en la región

Recolectar y procesar información sensible de las personas, como es la relativa a su condición de salud y a sus movimientos corporales, constituye una acción intrínsecamente riesgosa para las titulares de esos datos. Pero en lo relativo a aplicaciones, existen principios que pueden aplicarse para prevenir buena parte de ese daño. Como relata Sursiendo, hay ya grupos de investigación dedicados al desarrollo de aplicaciones y protocolos de seguimiento respetuosos de la privacidad, y cabe a los gobiernos tanto hacer eco de las preocupaciones de la sociedad civil como recoger y apoyar tales iniciativas. Los requerimientos delineados por el Chaos Computer Club para las aplicaciones son un punto de partida crucial para ese desarrollo.

Por cierto, el desarrollo tecnológico por si solo está condicionado por factores sociales, incluyendo los normativos, que sirven como garantía al respeto a los derechos fundamentales. Como hemos indicado, es también posible recurrir a legislación de emergencia no para facilitar la acción del estado vigilante, sino para asegurar el pleno respeto de los derechos de las personas afectados por la recolección y uso de su información personal. Además de ese rol protector, la regulación puede así procurar la prevención de que el estado de excepción se convierta en el de normalidad, y que la vigilancia pueda extenderse mucho más allá de la emergencia actual, incluso con aprobación popular producto de una distorsionada percepción de la realidad.

Pero además del deber de discutir apropiadamente cómo utilizar la tecnología que involucra vigilancia, es relevante discutir también el porqué. ¿Por qué es la vigilancia una posibilidad de acción percibida como “necesaria”, cuando ni siquiera su carácter de conveniente es inconcusso? ¿Por qué justificar, y finalmente normalizar, que bajo ciertas condiciones sea aceptable monitorear nuestras expresiones, o llenar nuestros cuerpos, hogares y poblados con cámaras, georreferenciación, reconocimiento facial, detección de calor, reportes voluntarios de salud, y más? El no despliegue de la acción vigilante del Estado es también una opción, especialmente de cara a los riesgos involucrados y de la existencia de medidas de salud pública con un impacto comprobadamente mayor. Insistir en soluciones tecnológicas puede llevarnos a eludir discusiones más profundas sobre fallas sistémicas que no son causadas por virus o desastres naturales, sino por decisiones políticas sobre la organización de la economía y de la vida en sociedad. ■

Fuente: [DerechosDigitales](#). 01 de mayo, 2020. CC BY-SA 3.0 CL

Juan Carlos Lara es parte de Derechos Digitales desde 2008 y actualmente coordina el equipo de investigación y políticas públicas de la organización. Anteriormente se desempeñó como investigador en temas vinculados a la propiedad intelectual, la libertad de expresión, el acceso al conocimiento y la labor académica en el entorno digital.

# The Girona Manifesto on Linguistic Rights

*Sixty-one NGOs, 41 PEN Centres and 40 experts in linguistic rights from all over the world met in Barcelona, 6-8 June 1996. The convocation of the World Conference on Linguistic Rights (WCLR) was an initiative of the Translations and Linguistic Rights Commission of PEN International and the CIEMEN (Centre Internacional Escarré per a les Minories Ètniques i les Nacions) with the moral and technical support of UNESCO.*

The Assembly of Participants at the WCLR approved the [Universal Declaration of Linguistic Rights](#) (UDLR) in a ceremony held in the Auditorium of the University of Barcelona, presenting the signed document Mr. Andri Isaksson, official representative of the UNESCO Director General.

Five years later, the Translation and Linguistic Rights Committee developed the Girona Manifesto on Linguistic Rights in 2011 as a tool to aid the dissemination and implementation of the UDLR. PEN Centres around the world have assisted in translating it into over 30 languages.

The Translation and Linguistic Rights Committee believes that translation is inseparable from linguistic rights and that the work of translators is central to the promotion of the right of all linguistic communities to be treated as equal. PEN is committed to an understanding of translation wherein all literatures, no matter how they are defined, enrich one another.

The Girona Manifesto is a ten-point document designed to be translated and disseminated widely as a tool to defend linguistic diversity

around the world. At PEN International's 77th annual Congress the PEN General Assembly approved the Manifesto.

PEN members have translated the Manifesto into various languages and encourage others to translate it into their own and to continue raising awareness about the need to protect and promote linguistic diversity. The Manifesto reads:

1. Linguistic diversity is a world heritage that must be valued and protected.
2. Respect for all languages and cultures is fundamental to the process of constructing and maintaining dialogue and peace in the world.
3. All individuals learn to speak in the heart of a community that gives them life, language, culture and identity.
4. Different languages and different ways of speaking are not only means of communication; they are also the milieu in which humans grow and cultures are built.
5. Every linguistic community has the right for its language to be used as an official language in its territory.
6. School instruction must contribute to the prestige of the language spoken by the linguistic community of the territory.
7. It is desirable for citizens to have a general knowledge of various languages, because it favours empathy and intellectual openness, and contributes to a deeper knowledge of one's own tongue.
8. The translation of texts, especially the great works of various cultures, represents a very important element in the necessary process of greater understanding and respect among human beings.
9. The media is a privileged loudspeaker for making linguistic diversity work and for competently and rigorously increasing its prestige.
10. The right to use and protect one's own language must be recognized by the United Nations as one of the fundamental human rights. ■

## European Charter for Regional or Minority Languages (1998)

*This treaty aims to protect and promote the historical regional or minority languages of Europe. It was adopted, on the one hand, in order to maintain and to develop the Europe's cultural traditions and heritage, and on the other, to respect an inalienable and commonly recognised right to use a regional or minority language in private and public life.*

First, it enunciates objectives and principles that Parties undertake to apply to all the regional or minority languages spoken within their territory: respect for the geographical area of each language; the need for promotion; the facilitation and/or encouragement of the use of regional or minority languages in speech and writing, in public and private life (by appropriate measures of teaching and study, by transnational exchanges for languages used in identical or similar form in other States).

Further, the Charter sets out a number of specific measures to promote the use of regional or minority languages in public life. These measures cover the following fields: education, justice, administrative authorities and public services, media, cultural activities and facilities, economic and social activities and transfrontier exchanges. Each Party undertakes to apply a minimum of thirty-five paragraphs or sub-paragraphs chosen from among these measures, including a number of compulsory measures chosen from a "hard core". Moreover, each Party has to specify in its instrument of ratification, acceptance or approval, each regional or minority language, or official

language which is less widely used in the whole or part of its territory, to which the paragraphs chosen shall apply.

Enforcement of the Charter is under control of a committee of experts which periodically examines reports presented by the Parties. ■

## Charte européenne des langues régionales ou minoritaires (1998)

*Ce traité prévoit la protection et la promotion des langues régionales et minoritaires historiques. Son élaboration est justifiée, d'une part, par le souci de maintenir et de développer les traditions et le patrimoine culturels européens, d'autre part, par le respect du droit imprescriptible et universellement reconnu de pratiquer une langue régionale ou minoritaire dans la vie privée et publique.*

Elle contient d'abord des objectifs et principes que les Parties s'engagent à respecter pour toutes les langues régionales ou minoritaires existant sur leur territoire : respect de l'aire géographique de chacune de ces langues, nécessité d'une promotion, facilité et/ou encouragement de leur usage oral et écrit dans la vie publique et privée (par des moyens adéquats d'enseignement et d'étude, par des échanges transnationaux pour ces langues qui sont pratiquées sous une forme identique ou proche dans d'autres Etats).

Ensuite, la Charte énumère toute une série de mesures à prendre pour favoriser l'emploi des

langues régionales ou minoritaires dans la vie publique. Ces mesures couvrent les domaines suivants : l'enseignement, la justice, les autorités administratives et les services publics, les médias, les activités et équipements culturels, la vie économique et sociale et les échanges transfrontaliers. Chaque Partie s'engage à appliquer au moins 35 paragraphes ou alinéas parmi ces mesures dont un certain nombre est à choisir obligatoirement parmi un "noyau dur". De plus, chaque Partie doit spécifier dans son instrument de ratification chaque langue régionale ou minoritaire répandue sur l'ensemble ou une partie de son territoire à laquelle s'appliquent les paragraphes choisis.

L'application de la Charte est contrôlée par un Comité d'experts qui est chargé d'examiner des rapports périodiques présentés par les Parties.

## Promotion and use of multilingualism and universal access to cyberspace (2003)

*The General Conference of UNESCO, recognizing the importance of promoting multilingualism and equitable access to information and knowledge, especially in the public domain, adopted the following Recommendation at its 32nd session (30 September – 17 October 2003).*

Through this Recommendation, which proposes measures fostering universal access to digital resources and services, and facilitating the preservation of their cultural and language diversity, UNESCO is encouraging its Member States to support equitable and affordable access

to information and to promote the development of a multicultural information society.

## **Development of Multilingual Content and Systems**

1. The public and private sectors and the civil society at local, national, regional and international levels should work to provide the necessary resources and take the necessary measures to alleviate language barriers and promote human interaction on the Internet by encouraging the creation and processing of, and access to, educational, cultural and scientific content in digital form, so as to ensure that all cultures can express themselves and have access to cyberspace in all languages, including indigenous ones.

2. Member States and international organizations should encourage and support capacity building for the production of local and indigenous content on the Internet.

3. Member States should formulate appropriate national policies on the crucial issue of language survival in cyberspace, designed to promote the teaching of languages, including mother tongues, in cyberspace. International support and assistance to developing countries should be strengthened and extended to facilitate the development of freely accessible materials on language education in electronic form and to the enhancement of human capital skills in this area.

4. Member States, international organizations and information and communication technology industries should encourage collaborative participatory research and development on, and local adaptation of, operating systems, search engines and web browsers with extensive multilingual capabilities, online dictionaries and terminologies. They should support international cooperative efforts with regard to automated translation services accessible to all, as well as intelligent linguistic systems such as those performing multilingual information retrieval, summarizing/abstracting and speech understanding, while fully respecting the right of translation of authors.

5. UNESCO, in cooperation with other international organizations, should establish a collaborative online observatory on existing policies, regulations, technical recommendations, and best practices relating to multilingualism and multilingual resources and applications, including innovations in language computerization.

## **Facilitating Access to Networks and Services**

6. Member States and international organizations should recognize and support universal access to the Internet as an instrument for promoting the realization of the human rights as defined in Articles 19 and 27 of the Universal Declaration of Human Rights.

7. Member States and international organizations should promote access to the Internet as a service of public interest through the adoption of appropriate policies in order to enhance the process of empowering citizenship and civil society, and by encouraging proper implementation of, and support to, such policies in developing countries, with due consideration of the needs of rural communities.

8. In particular, Member States and international organizations should establish mechanisms at the local, national, regional and international levels to facilitate universal access to the Internet through affordable telecommunications and Internet costs with special consideration given to the needs of public service and educational institutions, and of disadvantaged and disabled population groups. New incentives in this area should be designed towards this end including public-private partnerships to encourage investment and the lowering of financial barriers to the use of ICT, such as taxes and customs duties on informatics equipment, software and services.

9. Member States should encourage Internet service providers (ISPs) to consider provision of concessionary rates for Internet access in public service institutions, such as schools, academic institutions, museums, archives and public libraries, as a transitional measure towards universal access to cyberspace.

10. Member States should encourage the

development of information strategies and models that facilitate community access and reach out to all levels of society, including the setting up of community projects and fostering the emergence of local information and communication technology leaders and mentors. Strategies should also support cooperation on ICT among public service institutions, as a means of reducing the cost of access to Internet services.

11. Interconnection on a negotiated cost-sharing basis in the spirit of international cooperation should be encouraged between national Internet peering points combining the traffic of private and non-profit ISPs in developing countries and peering points in other countries whether developing or industrialized.

12. Regional organizations and forums should encourage the establishment of inter- and intra-regional networks powered by high capacity regional backbones to connect each country within a global network in an open competitive environment.

13. Concerted efforts within the United Nations system should promote the sharing of information about and experience on the use of ICT-based networks and services in socio-economic development, including open source technologies, as well as policy formulation and capacity-building in developing countries.

14. Member States and international organizations should promote appropriate partnerships in the management of domain names, including multilingual domain names.

## **Development of Public Domain Content**

15. Member States should recognize and enact the right of universal online access to public and government-held records including information relevant for citizens in a modern democratic society, giving due account to confidentiality, privacy and national security concerns, as well as to intellectual property rights to the extent that they apply to the use of such information. International organizations should recognize and promulgate the right for each State to have access to essential data relating to its social or eco-

nomic situation.

16. Member States and international organizations should identify and promote repositories of information and knowledge in the public domain and make them accessible by all, thus shaping learning environments conducive to creativity and audience development. To this end, adequate funding should be provided for the preservation and digitization of public domain information.

17. Member States and international organizations should encourage cooperative arrangements which respect both public and private interests in order to ensure universal access to information in the public domain without geographical, economic, social or cultural discrimination.

18. Member States and international organizations should encourage open access solutions including the formulation of technical and methodological standards for information exchange, portability and interoperability, as well as online accessibility of public domain information on global information networks.

19. Member States and international organizations should promote and facilitate ICT literacy, including popularizing and building trust in ICT implementation and use. The development of “human capital” for the information society, including an open, integrated and intercultural education combined with skills training in ICT, is of crucial importance. ICT training should not be limited to technical competence but should also include awareness of ethical principles and values.

20. Inter-agency cooperation within the United Nations system should be reinforced with a view to building up a universally accessible body of knowledge, particularly for the benefit of developing countries and disadvantaged communities, from the massive amount of information produced through development projects and programmes.

21. UNESCO, in close cooperation with other intergovernmental organizations concerned, should undertake the compilation of an

international inventory of legislation, regulations and policies on the generation and online dissemination of public domain information.

22. Definition and adoption of best practices and voluntary, self-regulatory, professional and ethical guidelines should be encouraged among information producers, users and service providers with due respect to freedom of expression.

### **Reaffirming the Equitable Balance between the Interests of Rights-Holders and the Public Interest**

23. Member States should undertake, in close cooperation with all interested parties, the updating of national copyright legislation and its adaptation to cyberspace, taking full account of the fair balance between the interests of authors, copyright and related rights-holders, and of the public embodied in international copyright and related rights conventions.

24. Member States and international organizations, when appropriate, should encourage rights-holders and the lawful beneficiaries of limitations and exceptions to copyright and related rights protection to ensure that such limitations and exceptions are applied in certain special cases that do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the rights-holders as required for in the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT).

25. Member States and international organizations should pay careful attention to the development of technological innovations and to their potential impact on access to information in the framework of copyright and related rights protection under international treaties and agreements. ■

# **Digital justice manifesto: A call to own our digital future**

## **Just Net Coalition**

*The Digital Justice Manifesto, “A Call to Own Our Digital Future”, was launched in Berlin in November 2019 by the Just Net Coalition, a global network of civil society organizations and individuals, including the World Association for Christian Communication. The coalition was founded at a meeting in New Delhi in 2014, which agreed “The Delhi Declaration for a Just and Equitable Internet”.*

### **Key Principles**

1. Data subjects must own their data – individually and collectively
2. Our data requires protection from abuse
3. We need the tools to control our data
4. Data commons need appropriate governance frameworks
5. Data protection and sharing require new regimes
6. Data-creating jobs ought to come with data rights
7. Data should be processed close to point of origin
8. Cross-border data flows must be decided nationally
9. Techno-structures need to be reclaimed as personal and public spaces
10. We own and should control our software
11. Key digital infrastructures need to be governed as public utilities
12. Techno-structures must be decentralised

- for open use, with interoperability
13. Global data monopolies should be broken
  14. Societies' datafication needs to be managed democratically
  15. Digital standards must be developed by public interest bodies
  16. The digital has to be governed in a local-to-global manner

## Preamble

We begin by endorsing and reaffirming [The Delhi Declaration for a Just and Equitable Internet](#). The present Manifesto builds on that Declaration and extends it.

### *A digital society is upon us*

People respond to the emerging digital future with a mixture of positive anticipation, awe, helplessness and even horror. Such a passive reaction to **society's most powerful driving force is both dangerous and unnecessary**.

There is no time to lose in taming the power of the digital. We can surrender our digital future, or we can take ownership of it. But first we must understand **what lies behind the digital**.

Industrialisation harnessed massive physical power from sources beyond those of people and animals, that transformed the processes of production. This is known as mechanisation. A digital economy and society is created by harnessing external (non-human) sources of 'intelligence power' i.e. the immense data-based intelligence that is revolutionising the forces of production. **This can be called the *intelligisation of socio-economic processes*.**

Colonisation bore horrific witness to how industrial power and the imperatives of capital were almost impossible to resist or challenge by those subjected to them. Yet **the power of others owning detailed intelligence about and over us**, and processing it through elaborate socio-economic systems to generate enormous profits through limitless manipulation, is perhaps worse than anything we have experienced so far.

### ***Data, intelligence and techno-structures***

Data must be recognised as a key economic resource. Currently, the resource of data gets globally appropriated at will; harvested without permission or recompense, and accumulated by data corporations for their exclusive use. We must choose whether to allow corporations to own **people's data, or if we, the people, should own it**. **The people, after all, are both the data contributors and data subjects**. Data corporations take advantage of default lawless practises of data accumulation and exclusive use; challenging them requires countervailing laws affirming people's rights and ownership over their data – both individual and collective.

Digital intelligisation was preceded and enabled by the spread of **networked software as the space, means and logic of our social, economic, political and cultural interactions and relationships**. The Internet was its first prototype. And because the Internet's core model was based on intelligence at the edges and on open, public protocols, it spawned a technical and social evolution that many believed would favour greater end-user control and decentralisation. Cloud computing – now the dominant networked software model – has **inverted that paradigm: controlling intelligence now lies with a few global centres, based largely on corporate control and ownership of data and private standards**. The ubiquitous spread of Internet-based cloud applications enables the collection of the most intimate and granular real-time data about us, the people. Such intensive and unrelenting data collection underpins and enables the powerful autonomous intelligence behind the phenomenon of digital society.

At the centre of intelligent digital systems are a few global businesses – 'intelligence corporations', whose services are based on digital intelligence or artificial intelligence (AI). They first connect, then coordinate, and ultimately control and dictate to all actors and activities in any sector – from transport and commerce to health and education. **They become the 'brain' of every sector**. Global intelligence corporations

operate **remotely through techno-structures of cloud computing**. Bypassing face-to-face human interactions, they thus avoid responsiveness and accountability, as well as legal and regulatory checks.

### **Taking back digital power**

Reclaiming power from ‘intelligence corporations’ requires people to work on two main fronts. First, **wrest back ownership of our personal and collective data and intelligence**. These are the key sources of digital power. Second, **take sufficient control over the techno-structures** within which data and intelligence operate. These techno-structures spread far, wide and deep into society, controlling and exploiting everything they reach. Unlike in the offline world where socio-economic interactions mostly take place in public or quasi-public spaces, in the digital world they are all enclosed within privately owned techno-structures.

Yet intelligent systems can operate productively and beneficially even when their intelligence, as well as the key nodes and pillars of their techno-structures, are distributed and collectively owned. It would involve employing the best possibilities of entrepreneurship and competitive markets, combined with critically important non-market collective mechanisms. **Such alternatives must be shaped at the same time that exploitative dominant models of centralised intelligence control are undone.**

The digital reshapes our social relationships and power structures so fundamentally that society’s **data and intelligence governance requires a new digital social contract**.

In our determination and struggle **to enable people to own their digital futures**, we adopt, and advocate, the following principles – towards a digital society that is just, equitable and sustainably productive.

### **People own their data and intelligence**

**1. Data subjects must own their data – individually and collectively:** Data about us, and intelligence about us, inherently belong to us – as in-

dividuals, and collectively as communities. Such data could directly be about people, or about things owned by or associated with them. Political, constitutional, and legal frameworks, at both national and international levels, must recognise and enforce this basic principle of data and intelligence ownership.

#### **2. Our data requires protection from abuse:**

The international human rights regime must recognise the inextricable interconnection between people and their data, and articulate benchmarks for safeguarding personal and collective data. Strong constitutional and legal protections are required against abuse of personal and collective data and intelligence, whether by corporations or the state. New laws and institutions are required for this purpose, that keep evolving to address emergent new risks.

**3. We need the tools to control our data:** The purpose of data and intelligence must not be to distinguish between people for unfair, discriminatory treatment, but to help and enable them to maximise digital benefits. Individuals and communities must be provided appropriate means to control their data, and apply it in ways best suited to their interests. Such means will both be individual and collective, requiring institutions that are adequate, practical and effective. It would involve well-regulated open markets and competitive businesses, as well as establishing new commons and public structures. This demands considerable institutional innovation.

**4. Data commons need appropriate governance frameworks:** Data commons and intelligence commons must be developed and treated as public goods. But data and intelligence cannot simply be open access resources; significant protections and circumscribing are essential. Being specific to particular individuals or groups and communities, unchecked access to, and use of, data and intelligence commons bear the potential for harm. In the manner that data actually gets employed by monopoly-prone businesses, data and intelligence commons are akin to ‘common pool resources’ – subject to overuse, depletion, congestion, rivalry and pollution. Requiring

regulated and calibrated use, data and digital intelligence must be subject to ‘common property regimes’, which calls for development of appropriate data and intelligence governance frameworks.

**5. Data protection and sharing require new regimes:** Innovative institutions should evolve for sharing of data and intelligence in a protected and regulated manner. Data institutions, such as data commons, data trusts, data infrastructures, and fair data markets, must be developed. As appropriate, these should involve mandated data sharing. Businesses and other entities have simultaneously to be provided sufficient incentives, within a public interest framework, for them to collect the necessary data and convert it into useful intelligence.

**6. Data-creating jobs ought to come with data rights:** Specific economic groups that make marked contributions to, and are key subjects of, data in a particular sector or an ‘intelligent system’, should have corresponding special data ownership rights. These could be drivers on a taxi platform, traders on an e-commerce platform, farmers on an agri-platform or workers in data-producing jobs. These groups should have primary economic rights – individual and collective – over the data they contribute. Such data constitutes the main value of the corresponding platform or intelligent system. Data-creating actors on a platform therefore have the right to participate in the governance of that platform, for example through adequate representation on the governing board. Alternatively, they may choose to pool their data to develop platform cooperatives, or a public or non-profit agency can help them to so organise.

**7. Data should be processed close to point of origin:** Important data will need to be localised in many cases. Data can be processed close to its point of origin, for which technologies already exist, and further innovations will emerge as society demands them. This can provide data subjects more effective control over their data. Necessary technical, policy and business models should be employed towards a local-to-global architecture

of digital services. In contrast to the current situation where digital activities on the ground are largely remote-controlled ‘satellite operations’ of a few global corporations, digital should have a pronounced local-ness and community control.

**8. Cross-border data flows must be decided nationally:** The data-owning national community must determine the terms on which cross-border flows of data may take place. Irrespective of its physical location, data should be subject to the *primary jurisdiction* of data’s country of origin. As personal data is an extension of one’s person-hood, so community data is an extension of community identity and being. Such primary jurisdiction involves not just privacy protections but also economic rights and ownership. Agreements among countries are required to mutually recognise, and help apply, *primary jurisdiction* over data – involving social, political and economic rights – of the country and community of origin of data. Regional groups that manage such inter-country agreements may gain mutual benefit from common data and digital spaces.

### People have rights to their digital techno-structures

**9. Techno-structures need to be reclaimed as personal and public spaces:** Networked software or cloud applications form the digital space, and the body of digital systems. These may be termed as the key digital techno-structures. They are currently almost entirely centralized and owned by a handful of corporations. Some, like those running heart pacemakers or mobile phones, penetrate deep into our otherwise personal realms; and others, like social networking, search, and transport applications, are analogous to what in the offline world are public spaces and structures, such as public streets, libraries and infrastructural services. Digital techno-structures’ essential personalness and publicness must be reclaimed and restored, where and as appropriate, from the existing state of their complete, end-to-end, corporate ownership and control.

**10. We own and should control our software:** People must fully own, and be able to control,

the software they install in their personal or collectively owned equipment. Technology Protection Measures are incursions upon people's basic rights. People should have the right to own, break-into, modify or remove, as they deem fit, whatever technical artefacts that exist within their personal or collective realms. This is a fundamental element of digital self-determination.

**11. Key digital infrastructures need to be governed as public utilities:** In the physical, offline world, non-personal, social and economic spaces and structures are divided between being public and belonging to private businesses. Infrastructure is normally public, or quasi-public, over and around which businesses may undertake their private activities. Digital spaces and structures require a similar arrangement. Key monopolistic digital infrastructures should be public utilities, even if provided by private businesses. This includes, as appropriate, computing platforms, search engines, social networks, email services, basic security systems, payment services, and e-commerce platforms.

**12. Techno-structures must be decentralised for open use, with interoperability:** Digital power can be redistributed by decentralising the techno-structures of connectivity, software, Internet, cloud computing, and AI applications/engines, while mandating interoperability. Such decentralisation is useful even where it entails some degree of immediate loss of efficiency. Apart from being more fair, decentralised digital power is more sustainably productive in the long term. Decentralised and open digital architectures include open community networks, open source software, open and neutral Internet, open and community data, and open and community AI. These can and must involve appropriate business models and entities. Any such open system should however duly protect the data and digital intelligence of the people and communities concerned, and affirm their right to self-determination.

**13. Global data monopolies should be broken:** National and international competition regimes, that are adequate to the new digital realities,

must break up vertically and horizontally integrated global digital structures. These regimes should aim at *ex ante* open, competitive and innovation-supporting digital market structures, and not just narrowly construed *ex post* consumer welfare that looks only at availability and price of services. The focus should be on cutting problematic links in data and intelligence value chains that underpin and promote digital monopolies. It may for instance be considered, where appropriate, to separate businesses that directly provide services to consumers, and collect their data, from businesses devoted specifically to technical services and general data processing and digital intelligence services.

### **The digital must be governed democratically, from local to global**

**14. Societies' datafication needs to be managed democratically:** Processes and areas facing or undergoing datafication and intelligisation require a three-way classification. Many kinds of datafication and intelligisation are just not desirable, whatever be the touted benefits. In other areas, while potentially useful in the long run, these processes may call for deliberate slowing down and close management, to deal with the possibilities of considerable short- to mid-term harm. Such harm could range from livelihood disruptions to requirements of considerable behaviour and cultural shifts that can be disorienting. Where datafication and intelligisation are evidently and immediately beneficial, people, and their representatives, should be in control of their implementation. These processes tend to have unanticipated, strong social consequences and must take place on democratically determined terms. A global human rights framework on data and intelligence governance should incorporate such a classification and corresponding due diligence.

**15. Digital standards must be developed by public interest bodies:** A major factor behind the current end-to-end digital control by a few digital corporations is the privatisation of digital standards development and non-enforcement of

interoperability. We must reclaim development of key digital technical standards exclusively by public interest bodies, and ensure strict compliance with them. These bodies should be appropriately representative of people, and based on public-interest oriented expertise. They should uphold the highest public and professional standards, be neutral and not aligned to any specific corporate or state interests, and fully eschew conflicts of interest.

16. *The digital has to be governed in a local-to-global manner:* Digital platforms provide services that have traditionally been largely developed and governed locally – like communication, media, commerce, transport, hotels, health and education. Having now become intelligence-driven does not necessarily mean that these services shed their localness. The required digital, data and intelligence governance structures and institutions will mostly be at national or local community levels, while some could be global. National polities still remain the anchors of self-determination and sovereignty of the people. Appropriate global governance of the digital should promote national and local digital economies. It ought to ensure that competitive, open, global technical services are accessible locally – including by local digital businesses – on fair, regulated terms. Digital governance must aim at a complete break with the current vertically-integrated global digital models – from concentrated intelligence or ‘brain’ centres in one or two countries of the world, right down to the last tiny ‘nerves’ that seek to control the smallest activity everywhere in a digital economy and society. A new digital model must be shaped that is local-to-global; that supports localness and furthers democratic self-determination, without compromising on the important benefits of the globalness of the digital. ■

# Manifeste pour une justice numérique : Appel à prendre en main notre avenir numérique

## Principes clés

1. Les sujets des données doivent être propriétaires de leurs données - individuellement et collectivement
2. Nos données doivent être protégées contre les abus
3. Nous avons besoin d'outils pour contrôler nos données
4. Les données communes ont besoin de cadres de gouvernance appropriés
5. La protection, le partage et l'utilisation des données nécessitent de nouvelles institutions
6. Tout travail créant des données doit s'accompagner de droits sur ces données
7. Les données devraient être traitées à proximité de leur point d'origine
8. Les flux transfrontières de données doivent être décidés au niveau national
9. Les technostuctures doivent être réappropriées en tant qu'espaces personnels et publics
10. Nous devrions être propriétaires de nos logiciels et être capables de les contrôler
11. Les infrastructures numériques clés doivent être régies en tant que services publics
12. Les structures technologiques doivent être décentralisées pour permettre une utilisation ouverte, avec interopérabilité
13. Les monopoles numériques mondiaux devraient être brisés
14. La numérisation des sociétés doit être gérée

démocratiquement

15. Les normes numériques doivent être élaborées par des organismes d'intérêt public

16. Le numérique doit être gouverné du local au global

## Préambule

Nous commençons par réaffirmer “La Déclaration de Delhi pour un Internet juste et équitable”. Le présent Manifeste s'appuie sur cette Déclaration et la prolonge.

### *Nous sommes à l'aube d'une société numérique*

L'avenir numérique émergeant est généralement accueilli avec un mélange d'anticipation positive, de crainte, d'impuissance et parfois d'horreur. **Une réaction aussi passive à l'égard de la force motrice la plus puissante de nos sociétés est à la fois dangereuse et inutile.**

Il n'y a pas de temps à perdre pour apprivoiser la puissance du numérique. Soit nous abandonnons notre avenir numérique, soit nous en prenons possession. **Mais nous devons d'abord comprendre ce qui se cache derrière le numérique.**

L'industrialisation a mobilisé une puissance physique massive à partir de sources extérieures aux humains et aux animaux qui a fini par transformer les processus de production. C'est ce qu'on appelle la mécanisation. De même, l'économie et la société numériques exploitent des sources externes (non humaines) de “pouvoir de renseignement”, sous la forme d'une immense intelligence basée sur les données, qui révolutionnent les forces de production. **C'est ce qu'on peut appeler “l'intelligencification” des processus socio-économiques.**

La colonisation a montré de la pire des manières comment le pouvoir industriel couplé aux impératifs du capital était presque impossible à résister ou à défier par ceux qui y étaient soumis. Or, **le pouvoir de ceux qui possèdent aujourd'hui des renseignements détaillés à notre sujet**, et qui les utilisent pour générer un contrôle économique et politique sans précédent,

est peut-être pire que tout ce que nous avons connu jusqu'à présent.

### *Données, intelligence et techno-structures*

Les données doivent être reconnues aussi comme une ressource économique essentielle. Actuellement, cette ressource fait l'objet d'une appropriation mondiale à volonté, elle est récoltée sans permission ou rétribution, et accumulée par des entreprises de données pour leur usage exclusif. **Nous devons choisir entre permettre à ces entreprises de posséder nos données ou bien en être propriétaires, nous, le peuple.** Après tout, **nous sommes à la fois les contributeurs et les sujets de ces données.** Les entreprises numériques profitent de l'absence de toute forme de droits économiques aux données pour ancrer leurs pratiques dans la loi par défaut. Il est urgent de mettre en place des régimes juridiques qui affirment les droits et la propriété des personnes sur leurs données - tant individuelles que collectives.

L’“intelligentification” numérique a été précédée et rendue possible par la diffusion **de logiciels en réseau devenus les espaces, moyens et logiques de nos interactions et relations sociales, économiques, politiques et culturelles.** L'Internet en a été le premier prototype. Comme son fondement était basé sur une intelligence périphérique et sur des protocoles publics ouverts, il a engendré une évolution technique et sociale qui, de l'avis de beaucoup, devait favoriser un plus grand contrôle de l'utilisateur final et une décentralisation. L'informatique en nuage (cloud computing) - actuellement le modèle dominant de logiciel en réseau - a inversé ce paradigme : **l'information est maintenant monopolisée par quelques centres mondiaux qui s'appuient sur le contrôle des données par les entreprises et sur des standards privés.** La diffusion omniprésente d'applications en nuage basées sur Internet permet la collecte ininterrompue, en temps réel, des données les plus intimes et les plus granulaires qui soient à propos de nous, le peuple. Voilà ce qui construit la puissante intelligence autonome derrière le phénomène de la société numérique.

Au centre des systèmes numériques intelligents se trouvent quelques entreprises mondiales - des "sociétés d'intelligence", dont les services sont basés sur l'intelligence numérique ou l'intelligence artificielle (IA). Ces sociétés commencent par connecter, puis coordonner, et finalement contrôler tous les acteurs et toutes les activités d'un secteur donné - des transports et du commerce à la santé et à l'éducation. **Elles deviennent le "cerveau" de chaque secteur.** Elles **opèrent à distance à travers des techno-structures d'informatique en nuage.** En contournant les interactions humaines en face à face, elles évitent de devoir rendre des comptes et d'assumer leurs responsabilités. Elles évitent aussi les contrôles légaux et réglementaires.

### ***Reprendre le pouvoir numérique***

Récupérer le pouvoir des mains des "sociétés d'intelligence" exige que nous travaillions sur deux fronts principaux. D'abord, **récupérer la propriété de nos données et de nos renseignements personnels et collectifs.** Ce sont les principales sources du pouvoir numérique. Deuxièmement, **obtenir un contrôle suffisant sur les technosstructures** au sein desquelles ces données et ces renseignements fonctionnent. Ces technosstructures s'étendent largement et profondément dans nos sociétés, contrôlant et exploitant tout ce qu'elles atteignent. Or, contrairement au monde hors ligne où les interactions socio-économiques se déroulent le plus souvent dans des espaces publics ou quasi-publics, dans le monde numérique, elles sont toutes enfermées dans des technosstructures privées.

Pourtant, les systèmes intelligents peuvent fonctionner de manière productive même lorsque leur intelligence, ainsi que les nœuds et les piliers clés de leurs technosstructures, sont distribués et détenus collectivement. Cela impliquerait d'utiliser au mieux les possibilités de l'esprit d'entreprise et des marchés concurrentiels, mais associés à des mécanismes collectifs non marchands d'une taille critique. **De telles alternatives doivent être élaborées en même**

**temps que les modèles exploiteurs dominants basés sur le contrôle centralisé de l'information sont détruits.**

Le numérique reconfigure si fondamentalement nos relations sociales et nos structures de pouvoir que **la gouvernance des données et de l'intelligence des sociétés exige un nouveau contrat social numérique.**

Dans notre détermination et notre lutte pour que les gens s'approprient leur avenir numérique, nous adoptons les principes suivants en faveur d'une société numérique juste, équitable et durable.

### ***Les gens sont propriétaires de leurs données et de leurs renseignements***

**1. Les sujets des données doivent être propriétaires de leurs données - individuellement et collectivement :** Les données nous concernant et les renseignements nous concernant nous appartiennent intrinsèquement à nous - en tant qu'individus et en tant que communautés. De telles données peuvent concerner directement des personnes ou des choses qui leur appartiennent ou qui leur sont associées. Les cadres politiques, constitutionnels et juridiques, tant au niveau national qu'international, doivent reconnaître et appliquer ce principe fondamental de la propriété des données et du renseignement qui en est issu.

**2. Nos données doivent être protégées contre les abus :** Le régime international des droits humains doit reconnaître le lien inextricable qui existe entre les personnes et leurs données, et définir des critères de référence pour la protection des données personnelles et collectives. Des protections constitutionnelles et juridiques solides sont nécessaires contre l'utilisation abusive des données et des renseignements personnels et collectifs de la part des entreprises ou des États. De nouvelles lois et de nouvelles institutions capables d'évoluer sans cesse pour faire face aux nouveaux risques sont nécessaires à cette fin.

**3. Nous avons besoin d'outils pour contrôler nos données :** L'objectif des données et des renseignements ne doit pas être de traiter

les personnes de manière injuste et discriminatoire, mais de les aider à maximiser les avantages du numérique. Les individus et les communautés doivent disposer des moyens appropriés pour contrôler leurs données et les utiliser de la manière la plus conforme à leurs intérêts. Ces moyens seront à la fois individuels et collectifs, nécessitant des institutions adéquates, agiles et responsables. L'innovation institutionnelle à cet égard nécessitera des marchés ouverts et bien réglementés garantissant la compétitivité des entreprises, ainsi que de nouveaux communs et structures publiques.

**4. Les données communes ont besoin de cadres de gouvernance appropriés :** Il est nécessaire d'élaborer des « communs » de données et de renseignements appropriés. Les données et le renseignement ne peuvent pas être simplement des ressources en libre accès. Pour éviter les abus, des limites et des protections sont essentielles. Dans la mesure où ces données et renseignements sont propres à des individus, des groupes ou des collectivités en particulier, un accès et une utilisation non contrôlés peuvent causer du tort. La façon dont les données sont utilisées les apparaît ainsi à un “commun” - sujet à la surexploitation, à l'épuisement, à la congestion, à la rivalité et à la pollution. Puisqu'une utilisation réglementée est nécessaire, les données et le renseignement numériques doivent être soumis à des “régimes de propriété commune”. Pour ce faire, il faut élaborer les cadres de gouvernance nécessaires en matière de données et de renseignements.

**5. La protection, le partage et l'utilisation des données exigent de nouvelles institutions :** Des institutions novatrices et solides sont nécessaires pour partager les données et les renseignements de manière protégée et réglementée. Il faut développer des institutions de données, telles que des patrimoines communs de données, des fiducies de données, des infrastructures de données et des marchés équitables des données. Ces institutions devraient également comprendre le partage obligatoire des données, si et où il y a lieu. Les entreprises et autres entités doivent bénéficier

simultanément d'incitations suffisantes, dans un cadre d'intérêt public, pour collecter les données nécessaires et les transformer en renseignements utiles.

**6. Tout travail qui crée des données doit s'accompagner de droits sur ces données :** Les groupes économiques qui contribuent de façon marquante aux données d'un secteur ou d'un “système intelligent” et qui en sont les principaux sujets, devraient bénéficier de droits de propriété spéciaux correspondants. Il peut s'agir des chauffeurs sur une plate-forme de taxi, de commerçants sur une plate-forme de commerce électronique, d'agriculteurs sur une plate-forme agricole ou de travailleurs dans des emplois producteurs de données. Ces groupes doivent bénéficier de droits économiques primaires - individuels et collectifs - sur les données qu'ils fournissent. Ces données constituent la principale valeur de la plate-forme ou du système intelligent correspondant. Les acteurs créateurs de données sur une plate-forme ont donc le droit de participer à la gouvernance de cette plate-forme, par exemple à travers une représentation adéquate au conseil d'administration. Alternativement, ils peuvent choisir de mettre en commun leurs données pour développer des plates-formes coopératives, ou encore une agence publique ou à but non lucratif peut les aider à s'organiser.

**7. Les données devraient être traitées à proximité de leur point d'origine :** Contrairement à la situation actuelle où les activités numériques locales relèvent en grande partie d’opérations par satellite” contrôlées à distance par quelques entreprises mondiales, le numérique doit avoir un caractère local et un contrôle communautaire prononcé. Dans de nombreux cas, des données importantes devront être localisées. Si les données sont traitées à proximité de leur point d'origine, les personnes concernées peuvent avoir un contrôle plus efficace sur leurs données. Les modèles techniques, politiques et commerciaux nécessaires devraient être utilisés pour développer une architecture de services de données et de services numériques qui aille du local au global. Des technologies existent déjà pour

le contrôle décentralisé des données et d'autres innovations verront le jour au fur et à mesure que la société les exigera.

**8. Les flux transfrontières de données doivent être décidés au niveau national :** La communauté nationale propriétaire des données doit déterminer les conditions dans lesquelles les flux transfrontaliers de données peuvent avoir lieu. Quel que soit leur emplacement physique, les données devraient être soumises à la juridiction principale de leur pays d'origine. De même que les données personnelles sont une extension de l'identité de la personne, les données communautaires sont aussi une extension de l'identité de la communauté. Cette compétence principale ne concerne pas seulement la protection de la vie privée, mais aussi les droits économiques et la propriété. Des accords entre pays sont nécessaires pour reconnaître mutuellement et pour aider à appliquer la juridiction primaire sur les données - y compris les droits sociaux, politiques et économiques - du pays et de la communauté d'origine des données. Les groupes régionaux qui parviennent à conclure de tels accords entre pays peuvent tirer un avantage mutuel de données et d'espaces numériques communs.

### **Les gens ont des droits sur leurs technostuctures numériques**

**9. Les technostuctures doivent être réappropriées en tant qu'espaces personnels et publics :** Les logiciels en réseau ou les applications en nuage forment l'espace du numérique et le corps des systèmes numériques. On peut les voir comme les principales technostuctures numériques. Elles sont actuellement presque entièrement centralisées et appartiennent à une poignée d'entreprises. Certaines, comme celles qui font fonctionner des stimulateurs cardiaques ou des téléphones mobiles, pénètrent profondément dans notre sphère personnelle ; d'autres, comme les réseaux sociaux ou les applications de recherche et de transport, sont analogues à ce qui, dans le monde hors ligne, relève d'espaces et de structures publics, comme les rues publiques, les bibliothèques ou les services infrastructurels. Le caractère per-

sonnel ou public, selon les cas, des technostuctures numériques doit donc être défendu contre leur appropriation et leur contrôle complets, de bout en bout, par des entreprises privées.

**10. Nous devrions être propriétaires de nos logiciels et être capables de les contrôler :** Les gens doivent être pleinement propriétaires des logiciels qu'ils installent sur leur équipement personnel ou collectif et être en mesure de les contrôler. Les mesures de protection technologique sont des atteintes aux droits humains fondamentaux. Les gens devraient avoir le droit de posséder, de modifier ou d'enlever, comme bon leur semble, tous les artefacts techniques qui existent dans leur domaine personnel ou collectif. Il s'agit d'un aspect fondamental de l'autodétermination numérique.

**11. Les infrastructures numériques clés doivent être régies en tant que services publics :** Dans le monde physique, les espaces et structures sociaux et économiques non personnels sont répartis entre le public et les entreprises privées. L'infrastructure est normalement publique, ou quasi-publique, les entreprises pouvant ensuite entreprendre leurs activités privées sur et autour d'elle. Les espaces et les structures numériques ont besoin d'un arrangement similaire. Les infrastructures numériques monopolistiques clés devraient être régies comme des services publics, même si elles sont fournies par des entreprises privées. Cela comprend, le cas échéant, les plates-formes informatiques, les moteurs de recherche, les réseaux sociaux, les services de courrier électronique, les systèmes de sécurité de base, les services de paiement et les plates-formes de commerce électronique.

**12. Les technostuctures doivent être décentralisées pour permettre une utilisation ouverte, avec interopérabilité :** La puissance numérique peut être redistribuée en décentralisant les technostuctures de connectivité, de logiciels, d'Internet, d'informatique en nuage et d'applications d'intelligence artificielle, tout en rendant obligatoire l'interopérabilité. Une telle décentralisation est utile même lorsqu'elle entraîne une relative perte d'efficacité immédiate. En plus

d'être plus équitable, une puissance numérique décentralisée est plus durablement productive à long terme. Les architectures numériques décentralisées et ouvertes comprennent des réseaux communautaires ouverts, des logiciels libres, un Internet ouvert et neutre, des données ouvertes et communautaires et des IA ouvertes et communautaires. Elles peuvent et doivent s'appuyer sur des modèles et des entités d'affaires appropriés. Tout système ouvert de ce type doit cependant dûment protéger les données et l'intelligence numériques des populations et communautés concernées et affirmer leur droit à l'autodétermination.

**13. Les monopoles numériques mondiaux devraient être brisés :** Les régimes de concurrence nationaux et internationaux adaptés aux nouvelles réalités numériques doivent briser les structures numériques mondiales intégrées verticalement et horizontalement. Ces régimes devraient viser des structures de marché numériques ouvertes, compétitives et favorables à l'innovation *ex ante*, et non pas seulement une interprétation construite *ex post* du bien-être des consommateurs qui ne porte que sur la disponibilité et le prix des biens et services. L'accent devrait être mis sur la suppression des liens problématiques dans les chaînes de valeur des données qui sous-tendent et favorisent les monopoles numériques. Il peut par exemple être envisagé de séparer les entreprises qui fournissent directement des services numériques aux consommateurs et qui collectent leurs données, des entreprises qui se consacrent spécifiquement aux services techniques et aux services généraux de traitement des données et de renseignement numérique.

### ***Le numérique doit être gouverné démocratiquement, du local au global***

**14. La numérisation des sociétés doit être gérée démocratiquement :** Les domaines confrontés ou en cours de "datafication" et d'"intelligencification" nécessitent une classification à trois niveaux. De nombreuses formes de "datafication" et d'"intelligencification" ne sont tout simplement pas souhaitables, quels que soient les avantages

qu'on leur prête. Dans d'autres domaines, bien qu'ils puissent être utiles à long terme, ces processus peuvent nécessiter un ralentissement délibéré et une gouvernance appropriée, afin de faire face aux risques de dommages considérables qu'ils posent à court et à moyen terme. Ces préjudices peuvent aller de la mise en cause de moyens de subsistance à l'exigence de changements comportementaux et culturels importants qui peuvent être désorientants. Enfin, là où la "datafication" et l'"intelligencification" sont manifestement bénéfiques à entreprendre immédiatement, les individus et leurs représentants devraient avoir le contrôle de leur mise en œuvre. Ces processus tendent à avoir de fortes conséquences sociales imprévues et doivent donc se dérouler dans des conditions déterminées démocratiquement. Un cadre mondial des droits humains sur la gouvernance des données et du renseignement devrait intégrer une telle classification, ainsi que la diligence raisonnable correspondante.

**15. Les normes numériques doivent être élaborées par des organismes d'intérêt public :** La privatisation des normes numériques et le non-respect de l'interopérabilité constituent un des principaux facteurs à l'origine du contrôle numérique de bout en bout exercé actuellement par un petit nombre de sociétés numériques. Nous devons exiger que le développement des normes techniques numériques clés soit exclusivement assuré par des organismes d'intérêt public et veiller au strict respect de ces normes. Ces organes devraient être fondés sur une expertise orientée vers l'intérêt public, sous le contrôle approprié des représentants du peuple. Les organismes d'élaboration de normes devraient respecter les normes publiques et professionnelles les plus élevées, être neutres et ne pas s'aligner sur des intérêts politiques ou corporatifs particuliers, et éviter tout conflit d'intérêts.

**16. Le numérique doit être gouverné du local au global :** Les plates-formes numériques fournissent des services qui ont traditionnellement été largement développés et régis localement - comme la communication, les médias, le commerce, les transports, les hôtels, la santé

et l'éducation. Le fait que ces services soient maintenant axés sur les données ne signifie pas qu'ils perdent leur caractère local. Les nouvelles structures et institutions nécessaires en matière de gouvernance du numérique, des données et du renseignement doivent se situer principalement au niveau des communautés nationales ou locales, tandis que certaines pourraient être mondiales. Les politiques nationales demeurent les piliers de l'autodétermination et de la souveraineté du peuple. Une gouvernance mondiale appropriée du numérique devrait promouvoir les économies numériques nationales et locales. Elle devrait veiller à ce que des services techniques mondiaux compétitifs et ouverts soient accessibles localement - y compris par les entreprises numériques locales - à des conditions équitables et réglementées. La gouvernance numérique doit viser à rompre complètement avec les modèles numériques mondiaux actuels, intégrés verticalement, depuis les centres de renseignement ou "cerveaux" concentrés dans un ou deux pays du monde, jusqu'aux derniers petits "nerfs" qui cherchent à contrôler la moindre activité partout dans l'économie et la société numériques. Un nouveau modèle numérique qui va du local au global doit être élaboré, qui soutienne le caractère local et favorise l'autodétermination démocratique, sans compromettre les avantages importants du caractère mondial du numérique. ■

*Pour endosser le manifeste, obtenir plus d'informations ou faire part de vos commentaires, écrivez à [info@justnetcoalition.org](mailto:info@justnetcoalition.org).*

# Manifiesto por la justicia digital: Un llamado para que nuestro futuro digital nos pertenezca

## Principios clave

1. Todas las personas deben tener potestad sobre sus datos, ya sea individual o colectiva.
2. Nuestros datos requieren protección contra el abuso
3. Necesitamos las herramientas para controlar nuestros datos
4. Los bienes comunes de datos requieren marcos de gobernanza adecuados
5. La protección, el intercambio y la utilización de datos requieren nuevas instituciones
6. El trabajo que genera datos debe ir acompañado de derechos digitales
7. Los datos deben procesarse cerca del punto de su origen.
8. Los flujos transfronterizos de datos deben regirse a nivel nacional
9. Es necesario reivindicar las tecno-estructuras como espacios personales y públicos
10. Deberíamos tener potestad sobre el software que utilizamos y poder controlarlo.
11. Las infraestructuras digitales clave deben ser administradas como servicios públicos
12. Las tecno-estructuras deben ser descentralizadas para un uso abierto, con interoperabilidad
13. Los monopolios digitales globales deben desarticularse
14. La datificación de las sociedades debe gestionarse democráticamente
15. El desarrollo de los estándares digitales debe ser la responsabilidad de organismos de interés público

16. La esfera digital debe ser gobernada de lo local a lo global.

## Preámbulo

Reafirmamos la “**Declaración de Delhi para una Internet justa y equitativa**”. El presente Manifiesto se basa en esta Declaración y la amplía.

### La sociedad digital ya está aquí

El futuro digital emergente es generalmente recibido con una mezcla de anticipación positiva, temor, impotencia e incluso horror. Esta reacción meramente pasiva ante la fuerza motriz más poderosa de la sociedad es peligrosa e innecesaria.

No hay tiempo que perder para controlar el poder de la esfera digital. O bien podemos renunciar a controlar nuestro futuro digital o podemos hacernos cargo de él. Pero primero debemos entender qué hay detrás de la esfera digital.

La industrialización aprovechó la potencia física masiva de fuentes más allá de las de las personas y los animales, hecho que transformó los procesos de producción. A este proceso se le conoce como mecanización. La economía y la sociedad digital se crean aprovechando fuentes externas (no humanas) del “poder de inteligencia”, en forma de una inmensa inteligencia basada en datos, que están revolucionando las fuerzas de la producción. Esto puede ser llamado como la “inteligencificación” de los procesos socioeconómicos.

La colonización fue un testimonio estremecedor de cómo el poder industrial, asociado con los imperativos del capital, ha sido casi imposible de resistir o de desafiar por parte de quienes estaban sujetos a él. Sin embargo, en la actualidad, el poder que detienen quienes poseen inteligencia detallada sobre nosotros y la emplean para generar un control económico y político sin precedentes, es quizás peor que todo lo que hemos experimentado hasta ahora.

### Datos, inteligencia y tecno-estructuras

Los datos deben ser reconocidos, entre otras cosas, como un recurso económico clave. En la actual-

idad, el recurso de los datos es apropiado globalmente a voluntad; es recolectado sin permiso ni recompensa, y es acopiado por las corporaciones de datos para su uso exclusivo. Debemos elegir entre permitir que las corporaciones sean propietarias de nuestros datos, o que éstos nos pertenezcan a nosotras, las personas. Las personas, después de todo, son tanto los contribuyentes como los sujetos de los datos. Las corporaciones de datos se aprovechan de la falta de derechos económicos reconocidos sobre los datos para afianzar sus prácticas de datos como ley de facto. Se necesitan urgentemente regímenes legales que afirmen los derechos y la potestad de las personas sobre sus datos, tanto individuales como colectivos.

La ‘inteligencificación’ digital fue precedida y facilitada por la difusión del software de red como el espacio, el medio y la lógica de nuestras interacciones y relaciones sociales, económicas, políticas y culturales. Internet fue su primer prototipo. Dado que el modelo básico de Internet se basaba en la inteligencia periférica o edge y en protocolos abiertos y públicos, dio lugar a una evolución técnica y social que muchas personas creían iba a favorecer la descentralización y mayor control por parte del usuario final. La computación en la nube –el modelo de software en red dominante en la actualidad– ha logrado invertir este paradigma: la inteligencia está ahora monopolizada por unos pocos centros globales, basados en el control corporativo de los datos y los estándares privados. La omnipresente difusión de las aplicaciones de Internet basadas en la nube, permite la recopilación incansable en tiempo real de los datos más íntimos y granulares sobre nosotros, las personas. Esto es lo que construye la poderosa inteligencia autónoma detrás del fenómeno de la sociedad digital.

En el centro de los sistemas digitales inteligentes, se encuentran unas pocas empresas globales –‘corporaciones de inteligencia’, cuyos servicios se basan en la inteligencia digital o inteligencia artificial (IA). Estas corporaciones primero conectan, luego coordinan y finalmente controlan a todos los actores y actividades en cualquier sector, desde el transporte y el comer-

cio, hasta la salud y la educación. Se convierten en el “cerebro” de cada sector. Las corporaciones globales de inteligencia operan de forma remota a través de las tecno-estructuras de la computación en la nube. Al pasar por alto las interacciones humanas cara a cara, evaden de esta forma su responsabilidad y la rendición de cuentas, así como los controles legales y reglamentarios.

## Recuperar el poder digital

Recuperar el poder de las ‘corporaciones de inteligencia’ requiere que trabajemos en dos frentes principales. En primer lugar, recuperar la potestad sobre nuestros datos e inteligencia, personales y colectivos. Estas son las fuentes clave del poder digital. Y, en segundo lugar, tomar el control suficiente sobre las tecno-estructuras dentro de las cuales operan los datos y la inteligencia. Estas tecno-estructuras se extienden a lo largo y ancho de la sociedad, controlando y explotando todo a su alcance. A diferencia de lo que ocurre en el mundo offline, donde las interacciones socioeconómicas tienen lugar principalmente en espacios públicos o quasi-públicos, en el mundo digital todas estas interacciones están encerradas dentro de tecno-estructuras de propiedad privada.

Sin embargo, los sistemas inteligentes pueden funcionar de forma productiva aun cuando su inteligencia, así como los nodos y pilares clave de sus tecno-estructuras, están distribuidos y son de propiedad colectiva. Esto implicaría emplear las mejores posibilidades del empresariado y de mercados competitivos, combinado con mecanismos colectivos no mercantiles de importancia crítica. Estas alternativas deben configurarse de manera paralela a la desarticulación de los modelos dominantes de explotación del control centralizado de la inteligencia.

La esfera digital remodela nuestras relaciones sociales y estructuras de poder de manera tan fundamental que la gobernanza de los datos y la inteligencia de la sociedad requiere un nuevo contrato social digital.

En nuestra resolución y lucha para que las personas puedan apropiarse de su futuro digital,

adoptamos los siguientes principios hacia una sociedad digital justa, equitativa y sosteniblemente productiva.

### Las personas tienen la potestad sobre sus datos e inteligencia

**1. Todas las personas deben tener potestad sobre sus datos, ya sea individual o colectiva:** Nuestros datos y la inteligencia que se genera a partir de ellos, nos pertenecen intrínsecamente – como individuos y como comunidades. Estos datos podrían ser directamente sobre personas, o sobre cosas que les pertenecen o están asociadas con ellas. Los marcos políticos, constitucionales y jurídicos, tanto a nivel nacional como internacional, deben reconocer y aplicar este principio básico de la pertenencia de los datos y de la inteligencia.

**2. Nuestros datos requieren protección contra el abuso:** El sistema internacional de derechos humanos debe reconocer la inextricable interconexión entre las personas y sus datos, y articular criterios básicos para salvaguardar los datos personales y colectivos. Se requieren de fuertes protecciones constitucionales y legales contra el abuso de los datos e inteligencia personales y colectivos, ya sea por parte de las empresas o del Estado. Para ello se necesitan nuevas leyes e instituciones que sigan evolucionando para hacer frente a los nuevos riesgos emergentes.

**3. Necesitamos las herramientas para controlar nuestros datos:** La finalidad de los datos y la inteligencia no deben ser utilizadas para separar a las personas, a través un trato injusto y discriminatorio, sino para ayudarles y permitirles maximizar los beneficios digitales. Los individuos y las comunidades deben disponer de medios adecuados para controlar sus datos y aplicarlos de la forma que mejor se adapte a sus intereses. Esos medios serán tanto individuales como colectivos y requerirán de instituciones adecuadas, ágiles y transparentes. La innovación institucional en este sentido requerirá mercados abiertos bien regulados que garanticen la competitividad de las empresas, así como nuevos bienes comunes y estructuras públicas.

**4. Los bienes comunes de datos requieren marcos de gobernanza adecuados:** Se requiere desarrollar bienes comunes de datos e inteligencia que sean adecuados. Pero los datos y la inteligencia no pueden ser simplemente recursos de acceso abierto. Para prevenir su abuso, los límites y las protecciones son esenciales. Siendo específicos a individuos o grupos y comunidades particulares, el acceso y el uso incontrolado de los bienes comunes de datos e inteligencia pueden resultar perjudiciales. En las formas en que los datos son empleados en la práctica por las empresas digitales, los bienes comunes de datos e inteligencia se asemejan a los “recursos de uso común”, susceptibles a un uso excesivo, agotamiento, congestión, rivalidad y contaminación. Los datos y la inteligencia digital requieren de regulación para su uso y deben estar sujetos a “regímenes de propiedad común”. Esto apela al desarrollo de los marcos de gobernanza necesarios en materia de datos e inteligencia.

**5. La protección, el intercambio y la utilización de datos requieren nuevas instituciones:** Se necesitan instituciones innovadoras y robustas para proteger y regular el intercambio de datos e inteligencia. Se debe crear instituciones de datos, como los bienes comunes de datos, fideicomisos de datos, infraestructuras de datos y mercados justos de datos. Estas también deberían implicar el intercambio obligatorio de datos, según y dónde sea apropiado. Las empresas y otras entidades deben contar simultáneamente con incentivos suficientes, dentro de un marco de interés público, para que recopilen los datos necesarios y los procesen para convertirlos en inteligencia útil.

**6. El trabajo que genera datos debe ir acompañado de derechos sobre los datos:** Los grupos económicos específicos que contribuyen notablemente a los datos de un sector particular o de un “sistema inteligente”, y que son sujetos clave de los mismos, deberían tener los correspondientes derechos especiales de potestad sobre de los estos datos. Podría tratarse de conductores en una plataforma de taxis, comerciantes en una plataforma de comercio electrónico, agricultores en una plataforma agrícola o trabajadores en em-

pleos de producción de datos. Estos grupos deben tener derechos económicos primordiales—individuales y colectivos—sobre los datos que aportan. Estos datos constituyen el valor principal de la plataforma o sistema inteligente correspondiente. Por lo tanto, los actores que crean datos en una plataforma tienen derecho a participar en la gobernanza de la misma, por ejemplo, mediante una representación adecuada en el consejo de administración. Alternativamente, pueden optar por poner en común sus datos para desarrollar plataformas cooperativas, o bien alguna agencia pública o sin fin de lucro podría ayudarles a organizarse en tal sentido.

**7. Los datos deben procesarse cerca del punto de su origen:** A diferencia de la situación actual, en la que las actividades digitales en el terreno son en gran medida ‘operaciones remotas’ controladas a distancia por unas pocas empresas mundiales, de hecho se debería rescatar su carácter netamente local, con control comunitario. En muchos casos, será necesario relocalizar los datos más importantes. Si los datos se procesan cerca de su punto de origen, los interesados pueden tener un control más efectivo de sus datos. Deberían emplearse los modelos técnicos, políticos y empresariales necesarios para lograr una arquitectura de datos y servicios digitales con una orientación de lo local a lo global. Ya existen tecnologías para el control descentralizado de datos y, a medida que la sociedad lo exija, surgirán nuevas innovaciones.

**8. Los flujos transfronterizos de datos deben regirse a nivel nacional:** La comunidad nacional de donde provienen los datos debe determinar las condiciones en las que pueden tener lugar los flujos transfronterizos de datos. Independientemente de su ubicación física, los datos deben estar sujetos a la jurisdicción primordial de su país de origen. Así como los datos personales son una extensión de la persona, también los datos de la comunidad son una extensión de la identidad y del ser comunitarios. Esta jurisdicción primordial involucra no sólo la protección de la privacidad, sino también los derechos y la potestad económicos. Se requiere establecer ac-

uerdos entre países para reconocer mutuamente y ayudar a aplicar la jurisdicción primordial sobre los datos –en relación a derechos sociales, políticos y económicos– del país y de la comunidad donde los datos tienen su origen. Los grupos regionales que logren concertar tales acuerdos entre países podrían sacar beneficio mutuo de los datos y los espacios digitales comunes.

### **Las personas tienen derechos a sus tecno-estructuras digitales**

**9. Es necesario reivindicar las tecno-estructuras como espacios personales y públicos:** El software en red o las aplicaciones en la nube conforman el espacio digital y el cuerpo de los sistemas digitales. Estos pueden ser considerados como las tecno-estructuras digitales clave. Actualmente, están casi totalmente centralizadas y son propiedad de un puñado de corporaciones. Algunas, como las que manejan marcapasos o teléfonos móviles, penetran profundamente en nuestro ámbito personal; y otras, como las redes sociales o las aplicaciones de búsqueda y transporte, son análogas a lo que en el mundo offline son los espacios y estructuras públicos, como las calles públicas, las bibliotecas y los servicios de infraestructura. Es necesario rescatar el carácter personal o público de las tecno-estructuras digitales de su actual sometimiento total a la propiedad y control de las corporaciones, en toda la cadena.

**10. Deberíamos tener la potestad sobre el software que utilizamos y poder controlarlo:** Las personas deben ser titulares plenos del software que instalan en sus equipos personales o colectivos, y poder controlarlo. Las Medidas de Protección de la Tecnología afectan los derechos básicos de las personas. Las personas deben tener derechos de tenencia, intervención, modificación o eliminación, según su criterio, en los artefactos técnicos que existen en su ámbito personal o colectivo. Este es un aspecto fundamental de la autodeterminación digital.

**11. Las infraestructuras digitales clave deben ser gobernadas como servicios públicos:** En el mundo físico, los espacios y estructuras

impersonales, sociales y económicos se distribuye entre la propiedad pública y la de empresas privadas. La infraestructura es normalmente pública, o quasi-pública, y sobre o alrededor de ella las empresas pueden llevar a cabo sus actividades privadas. Los espacios y estructuras digitales requieren una disposición similar. Las infraestructuras digitales monopólicas clave deben ser gobernadas como servicios públicos, incluso si son suministradas por empresas privadas. Ello incluye, según el caso, plataformas informáticas, motores de búsqueda, redes sociales, servicios de correo electrónico, sistemas de seguridad básica, servicios de pago y plataformas de comercio electrónico.

**12. Las tecno-estructuras deben ser descentralizadas para un uso abierto, con interoperabilidad:** La potencia digital puede redistribuirse al descentralizar las tecno-estructuras de conectividad, software, Internet, computación en nube y aplicaciones de IA, al tiempo que se exige la interoperabilidad. Esta descentralización es útil, incluso cuando conlleva cierto grado de pérdida inmediata de eficiencia. Además de ser más justa, el poder digital descentralizado es más productivo a largo plazo. Las arquitecturas digitales descentralizadas y abiertas incluyen redes comunitarias abiertas, software de código abierto, una Internet abierta y neutral, datos abiertos y comunitarios, y la IA abierta y comunitaria. Estos pueden y deben involucrar modelos de negocio y entidades apropiados. Sin embargo, cualquier sistema abierto de este tipo debe proteger debidamente los datos y la inteligencia digital de las personas y comunidades concernidas, y afirmar el derecho a la autodeterminación de éstas.

**13. Los monopolios digitales globales deben desarticularse:** Los regímenes de competencia nacionales e internacionales, adecuados a las nuevas realidades digitales, deben romper las estructuras digitales globales integradas vertical y horizontalmente. Estos regímenes deberían aspirar a unas estructuras de mercado digital ex ante, abiertas, competitivas y que apoyen la innovación, y no sólo a un bienestar ex post del consumidor interpretado de forma restrictiva que



sólo tenga en cuenta la disponibilidad y el precio de los bienes y servicios. La atención debería centrarse en cortar los vínculos problemáticos en las cadenas de valor de datos e inteligencia que sostienen y promueven los monopolios digitales. Por ejemplo, se puede considerar, cuando proceda, la posibilidad de separar las empresas que prestan directamente servicios digitales a los consumidores y recogen sus datos, de las empresas dedicadas específicamente a los servicios técnicos y a los servicios generales de procesamiento de datos e inteligencia digital.

### La esfera digital debe ser gobernada democráticamente, de lo local a lo global

**14. La datificación de las sociedades debe gestionarse democráticamente:** Las áreas que se enfrentan o están siendo sometidas a la datificación y a la ‘inteligencificación’ requieren una clasificación de tres vías. Muchos tipos de datificación e ‘inteligencificación’ no son deseables, cualesquiera que sean sus beneficios. En otros ámbitos, aunque potencialmente útiles a largo plazo, estos procesos pueden requerir una ralentización deliberada y una gobernanza adecuada, para hacer frente a las posibilidades de que se produzcan daños considerables a corto y mediano plazo. Esos daños podrían ir desde perturbaciones de los medios de subsistencia hasta

los requerimientos de cambios significativos en el comportamiento y la cultura que pueden ser desorientadores. Cuando es evidente que la datificación y la ‘inteligencificación’ tendrán beneficios inmediatos, las personas y sus representantes deberían controlar su implementación. Tales procesos tienden a tener fuertes consecuencias sociales imprevistas y deben realizarse bajo modalidades democráticamente determinadas. Un marco mundial de derechos humanos sobre gobernanza de datos e inteligencia debería incorporar esa clasificación y la correspondiente diligencia.

**15. El desarrollo de los estándares digitales debe ser la responsabilidad de organismos de interés público:** Un factor significativo detrás del actual control digital de toda la cadena por parte de unas pocas empresas digitales es la privatización del desarrollo de normas digitales y la no aplicación de la interoperabilidad. Debemos reclamar que el desarrollo de normas técnicas digitales clave sea exclusivo de organismos de interés público, y garantizar el estricto cumplimiento de dichas normas. Estos organismos deberían basarse en conocimientos especializados orientados al interés público, bajo la supervisión adecuada de los representantes de la población. Los organismos encargados de la elaboración de estándares deben respetar las más excelentes normas públicas y profesionales, ser neutrales y no estar alineados con ningún interés

empresarial o político específico, y evitar por completo los conflictos de intereses.

**16. La esfera digital debe ser gobernada de lo local a lo global:** Las plataformas digitales proporcionan servicios que tradicionalmente han sido desarrollados y gobernados localmente, como la comunicación, los medios de comunicación, el comercio, el transporte, los hoteles, la salud y la educación. El hecho de que ahora se hayan convertido en servicios basados en la inteligencia no significa necesariamente que estos servicios se despojen de su carácter local. Las nuevas estructuras e instituciones necesarias para la gobernanza de la esfera digital, los datos y la inteligencia se ubicarán, en su mayoría, a nivel nacional o de las comunidades locales, si bien algunas podrían ser globales. Las entidades nacionales siguen siendo los anclajes de la libre determinación y la soberanía del pueblo. Una gobernanza mundial adecuada de la esfera digital debería promover las economías digitales nacionales y locales. Debería garantizar que los servicios técnicos mundiales competitivos y abiertos sean accesibles localmente –incluido para las empresas digitales locales– en condiciones justas y reguladas. La gobernanza digital debe aspirar a una ruptura total con los actuales modelos digitales mundiales integrados verticalmente, desde los centros concentrados de inteligencia o ‘cerebros’ ubicados en uno o dos países del mundo, hasta los últimos y diminutos ‘nervios’ que tratan de controlar la actividad más pequeña en todas partes, en la economía y la sociedad digitales. Un nuevo modelo digital de lo local a lo global debe ser configurado, que apoye lo local y promueva la autodeterminación democrática, sin comprometer los importantes beneficios de la globalidad de la esfera digital. Proponemos estos principios como base para una nueva arquitectura de gobernanza de una sociedad digital justa y humana. ■

*Para suscribir el manifiesto, solicitar mayor información o enviar comentarios, escribir a [info@justnetcoalition.org](mailto:info@justnetcoalition.org)*

# Data as public good, and the public sector

Parminder Jeet Singh

*Understanding the nature of the emerging digital economy and society, and recognising people's collective rights to their data, can help to determine how society's data and digital intelligence-based roles should be divided across public, community and private sectors.*

The currently dominant models of digital technology, economy, and society were born and developed at a place and time of ascendant neoliberal ideology, namely in the US of the decades of 1990s and 2000s. These models are consequently almost entirely ruled by the private sector, with practically no role for the public sector. Given the need for rapid innovation and disruption at the early stages of digital technology application, private sector leadership may have had some justification. But with the digital society structures becoming entrenched now, and increasingly dominating all sectors, public sector's appropriate role in a digital society warrants assessment.

Key digital transportation data being largely in the hands of a few digital corporations, some cities in the US have considered handing over practically the entire public transportation sector to private management. Massive AI-based private education projects may push into oblivion the school system as we know it, and along with it also the educational authorities. Corporations holding health data are set to reorganise the health sector supplanting the role of public health systems. Digital corporations are developing smart city projects in which their control over city data converts into de facto governance of the city.

Not just provision of services, the very acts of public policy-making and governance would soon be impossible without access to society's digital data. Most of such data currently remains a private resource of digital corporations. They may pro bono share some of their data for purposes of public interest, for example, Facebook's »Data for Good« and Uber's »Uber Movement« initiatives. But such sharing obviously happens on the whims and terms of these corporations, and follows their own interests. It can hardly serve as the basis for how public policy and governance are to be undertaken in the digital age.

Let us consider a city that is planning smart traffic management, which will require access to real-time commuting data that mostly is only available with Google. Would the city authorities have to beg Google for this data or, as the dominant data economy model becomes mainstream and »accepted«, have to buy it? Even more likely, they may have to let Google, or some such digital corporation, manage city traffic services. This will involve monopoly service fees and lock-ins. Leveraging their new position, as the corporation involved gathers ever more city data, it will use it to forever keep improving its services and increasing the fees. Such a situation of irretrievable lock-in and ever-deepening dependence on a private provider for a public service may *prima facie* look entirely untenable, but that is where we seem to be imminently headed. This traffic management example can be extrapolated to every single area of public sector work, from city planning, community development and welfare services to utilities management, education, health, agriculture support, and more.

A central role of community data for a whole range of services that have traditionally been provided by the public sector points to the immense, and indispensable, public value of such data.<sup>1</sup> It makes a compelling case for community ownership of this data. Such ownership can enable free access to community data held by private companies whenever needed for purposes of public interest.<sup>2</sup> This arrangement in fact appears absolutely necessary, unless the public sector is

soon to more or less collapse completely. While data required for directly providing public services can be called as a core public interest need, other kinds of public interests are also relevant. Two such further purposes of public interest that require mandated sharing of data are (1) to ensure an open and competitive market for digitally intelligent products and services, and (2) to support domestic digital industrialisation.<sup>3</sup>

Is the public sector ready for new data-based roles? An appropriate theory about such roles for the public sector, and the enabling policies and laws like on community data ownership, are certainly needed first. But equally important are the practical details.

Much of the change and restructuring will take place within existing public sector bodies and institutions, like those providing services of transportation, health, education, welfare, etc. These bodies will have to become adept at collecting and curating the required data from their existing activities, as well as privately held data that they will get access to under community data ownership rules. Competencies will have to be developed to convert data into necessary digital intelligence, and use it to provide intelligent public services (of course with the help of data scientists). Considerable skill development and upgrading may be required for public sector workers, including bringing in new technical skills. But, at its core, digitalisation and datafication of the public sector is not so much of a technical challenge as often feared as it is of strategic visioning and able management. Public sector workers should be able to adapt to new data-intensive work processes as successfully they did to computerisation in the public sector many years ago.

Some of the required public sector restructuring may be relatively intensive, even if undertaken gradually to accommodate human and other kinds of costs. Some public-sector roles may indeed become less important in the digital society, but many entirely new ones will emerge.

With industrialisation, the public sector acquired the important role of providing key in-

dustrial infrastructure. It should be taking up a similar role with regard to digital infrastructure. If any such new role for the public sector is hardly ever discussed it owes largely to the digital society's birth and upbringing in a neoliberal environment. Global, vertically integrated digital corporations, spanning several sectors of the economy, internalise what are appropriately infrastructural and public-sector roles. Not only are the new digital infrastructure roles private right from birth – a creeping acquisition of existing public infrastructure roles is also taking place. An illustration of this is private digital currency initiatives like Facebook's Libra seeking to take over the government role of managing currency as the token of value in economic exchanges.<sup>4</sup>

New digital infrastructure areas range from digital connectivity and basic computing facilities to cloud computing and data provisioning.<sup>5</sup> As the very basis for intelligent production – of intelligent products and services – data is required for all important digital economy activities. Being in the nature of information, data is *prima facie* a non-rival good. Also, as data is combined with other data its value increases dramatically. This makes a case for provision of important data as a common infrastructure to all digital economy actors in any sector. The current digital economy model, however, is based on exclusive appropriation of society's data by a few monopolistic digital corporations. They thus increasingly control the value chains in all sectors. Such exclusive use of the common resource of society's data is the main reason for increasing concentration of digital power, and to a good extent also of increasing economic and social inequalities. Data sharing, or providing data as a common infrastructure, maximises the benefits that a society can derive from data. Sufficient open availability of key data is also the *sine qua non* for a competitive digital economy, and for reversing the damage being caused by concentration of digital power in a few hands.

The concept of data infrastructure is drawing increasing attention.<sup>6</sup> This differs from the earlier open data movement, which consisted mostly of

putting public data out in the open for anyone to use. Key data in different sectors mostly used to be with the public authorities; but today private digital platforms are the biggest holders of such data. Furthermore, digital society's granular and intrusive digital data is of a nature that requires considerable protection against misuse. Such data has to be shared in a regulated and managed manner.<sup>7</sup> Data infrastructures are designed for safe sharing of sector-wide data taken from different sources.

Command over AI is the new basis of economic power.<sup>8</sup> Various national AI strategies rightly focus on data availability, which requires data sharing.<sup>9</sup> They promote institutions like data infrastructures, data trusts, data exchanges and data markets, in order to ensure increased access to data for digital economic actors. Although mandated data sharing does get mentioned in some places, these national strategies mostly discuss voluntary data sharing. It is not explained, however, why the biggest collectors of data – digital platform companies – will on their own share or even sell their data when they consider maintaining exclusive access to data to be their main business advantage. In pussy-footing the obvious need for mandated data sharing, the frames of these national AI strategies seem to be tactically avoiding too direct a confrontation with the dominant political economy of the digital society, backed as it is by the most powerful global economic and political interests. But since effective data access and data sharing lie at the heart of any possibilities for AI and digital industrialisation, this weakness ensures that these AI strategies are doomed to failure in their current forms.<sup>10</sup>

Data infrastructures are not ordinary optional projects that can provide certain benefits; they constitute the very foundation of a strong domestic digital and AI industry, and ensure its openness and fairness. Data's privatisation and monopolistic appropriation, on the other hand, is at the core of the dominant digital economy model. There is no escaping this paradox; it needs to be squarely addressed and urgently resolved.

Public data infrastructures have to be a key part of the new digital institutional ecologies. Most of them will be directly run by the public sector as a part of existing public departments or agencies in different areas, or will be operated by setting up new cross-sectoral agencies. Some data infrastructures could be managed in partnerships with non-profits or businesses, and others run privately as regulated utilities. Effective regulation for data markets is also required. Public sector capacities need to evolve for all these roles.

Public data infrastructures in different sectors – commerce, transportation, finance, tourism, agriculture, health, education, the labour market, and so on, are necessary to (1) deliver respective intelligent public services, and (2) robust private sector development, supporting a host of competitive digital businesses in each area.<sup>11</sup> Data infrastructures play a central role in digital industrialisation, especially by nurturing domestic businesses.<sup>12</sup> When intelligent products and services are competitively available, and lock-ins made difficult with effective data-portability laws, it enables better distribution of digital power across an economy and society, as well as globally. This can ensure the best value for consumers, and greater bargaining power for workers and other small actors in digital supply chains.

India is developing public data infrastructures in many sectors, ranging from commerce and finance to health, education and agriculture.<sup>13</sup> The EU is creating data exchanges in the areas of transport,<sup>14</sup> logistics,<sup>15</sup> and health,<sup>16</sup> and a common database of health images to support AI applications in healthcare.<sup>17</sup> Similar initiatives are cropping up all over the world. Public data infrastructures will in time further specialise and evolve to provide not just raw or semi-structured data, but also its higher derivative forms. These could range from structured data and trained AI models to actual AI as a (public) service.<sup>18</sup>

Much discussion gets devoted nowadays to speculation over »AI versus humans«. But the most important political and economic question currently is: Who owns and controls society's AI systems, or »systemic intelligence about us«? This

is granular, real-time intelligence about – and thus nearly absolute power over – every niche and element of our socio-economic organisation. Is it with a handful of actors? Should we all not own it collectively? (Although uses of such digital intelligence, in many acceptable areas, will certainly need to be licensed under regulated conditions to private businesses for greatest productivity.) Our collective ownership over systemic digital intelligence about ourselves, as well as over the data from which it is derived, implies that a society's data and digital intelligence are to be public goods.

Striking at the heart of the default dominant model, such a public goods perspective provides us with a new point of departure towards a digital economy and society that is just, fair and equitable. It will take forward the mixed economy and welfare state models that characterised the dominant post-war consensus,<sup>19</sup> but have been upstaged by the neoliberal assault.<sup>20</sup> The latter has employed the cover of rapid digital flux to gain much new territory with respect to society's systems and institutions. If properly conceptualised, strategised and politicised, the same digital shift can in fact be leveraged to rehabilitate the pre-neoliberal consensus. This is because the key resources of the digital economy data and digital intelligence have some inherent features of a »social commons«.<sup>21</sup> ■

*Excerpted from [Economic Rights in a Data-Based Society: Collective Data Ownership, Workers' Rights, and the Role of the Public Sector](#), a paper published by the Friedrich-Ebert-Stiftung (2020) examining the fundamental changes taking place to economic structures, centred on the key digital economy resource of data, and exploring the implications of these changes for the public sector and its workers.*

#### Notes

1. Public value refers to the value created by government through services, laws, regulation and other actions. <https://www.themandarin.com.au/104843-measuring-public-value/>
2. India's AI strategy refers to mandatory data sharing for purposes of public interest , and some EU policy documents are also beginning to veer towards this view.
3. India's earlier referred draft e-commerce policy proposes such data.
4. <https://www.cnet.com/news/facebook-libra-cryptocurrency/>

5. The EU has infrastructural projects in areas of high-performance computing and low-power micro-processors required for large data and AI applications. <https://ec.europa.eu/11ewsroom/dae/document>
6. <https://www.stateofopendata.od4d.11et/chapters/issues/data-infrastructure.html>
7. »Open data« is in general useful, with little potential for harm. Digital economy data provides granular intelligence on specific individuals and groups and may carry great potential for harm. It therefore cannot just be made open to anyone and everyone without protections.
8. Russian President Vladimir Putin has observed that whoever takes the lead in AI will become the ruler of the world. This corresponds to leadership in industrialisation in an earlier era. <https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-theworld>
9. UK's AI strategy at <https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal>; India's at [https://www.niti.gov.in/writereaddata/files/document\\_publication/NationalStrategy-for-AI-Discussion-Paper.pdf?utm\\_source=hrintelligencer](https://www.niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf?utm_source=hrintelligencer); and France's.
10. The paths adopted by the US, as the first starter, and China, which thoroughly fire-walled its nascent digital economy, are generally not available at this stage to other countries for digital industrialisation.
11. See the chapter on "Public data infrastructures" in the paper "Digital industrialisation in developing countries". [https://itforchange.net/sites/default/files/1468/digital\\_industrialisation\\_in\\_developing\\_countries.pdf](https://itforchange.net/sites/default/files/1468/digital_industrialisation_in_developing_countries.pdf)
12. Ibid.
13. Ibid.
14. <https://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf>
15. <https://www.ieu.org/resources/newsroom/eu-digital-logisticsplatform-puts-e-cmr-test>
16. <https://ec.europa.eu/digital-single-market/en/exchange-electronic>
17. [https://ec.europa.eu/commission/presscorner/detail/fi/memo\\_18\\_6690](https://ec.europa.eu/commission/presscorner/detail/fi/memo_18_6690)
18. Al as a service« is an emerging business model. The public sector will need to move away from just using AI applications which co promises its hold over the value of very important data that passes through its hands and also specialise in providing some public-infrastructure AI services.
19. Somewhat arbitrarily, treating communism here as an exception.
20. Caught on the wrong foot by a bipolar digital world dominated by the US and China, EU leaders are beginning to think aloud in favour of such a »middle path« political economy for the digital society. <https://www.politico.eu/article/germanyfalling-behind-china-on-tech-innovation-artificial-intelligence-angela-merkel-knows-it/>
21. <http://datagovernance.org/report/data-a11d-data-intelligence->

Parminder Jeet Singh is Executive Director of [IT for Change](#). His engagements have been in the area of ICTs for development, Internet governance, e-governance, and digital economy.

# Media viability gets a boost

Lorenzo Vargas

*New models to fund and sustain the public interest media that the Internet disrupted are urgently needed. COVID-19 reminds us of just how pressing this need is.*

The notion of a free and independent media sector has always been one of the cornerstones of liberal democracy. The idea of a media sector that is free to serve as watchdog vis a vis the state and other powerful actors, as well as to inform citizens and provide platforms for expression is central to the idea of a society based on democratic principles.<sup>1</sup>

These ideas have been reproduced throughout the world in the actions of international NGOs, governments, and UN agencies. Many of these interventions have been guided by the principles of Freedom of the Press and Freedom of Expression, as well as by tools such as UNESCO's Media Development Indicators, which provide a framework to assess the extent to which media systems are independent and pluralistic.<sup>2</sup>

The emergence of the Internet as a key element of media ecosystems was initially received with much optimism by academics and practitioners. One such analysis proposed that the emergence of the Internet and social media platforms helped democratize media systems, allowing "citizens to report news, expose wrongdoing, express opinions, mobilize protest, monitor elections, scrutinize government, deepen participation, and expand the horizons of freedom."<sup>3</sup> This view was widely endorsed by the developments of the Arab Spring, in which activists used social media to help organize mass protests against authoritarian governments.<sup>4</sup>

Nevertheless, in recent years, there have been mounting concerns about the impact that

the use of Internet-based communication tools is having on democracies around the world. “One of the most significant and ongoing impacts of digital convergence on journalism is its effect on media viability and sustainability... Far too few news organizations have been able to find a sustainable model for journalism online, which translates into less revenue and fewer journalists. A diminished supply of reliable news media can also be seen as a core contributor to the ‘misinformation’ society.”<sup>5</sup>

A key element of this equation is the global advertising market, which has seen a shift away from being dominated by media companies and is now ruled by Internet companies such as Google and Facebook, which together have a market share of 63% - roughly USD \$61.6 billion per year. At the same time, global newspaper advertising revenue is expected to decline by USD 23.8 billion a year by 2021.<sup>6</sup> These concerns have been accompanied by growing threats to freedom of expression and freedom of the press in many countries, with Freedom House data showing that “freedom of expression [has been] declining each year over the last 13 years, with sharper drops since 2012...In 2018, press freedom scores fell in four out of six regions in the world.”<sup>7</sup>

The crisis brought about by the COVID-19 pandemic reminded us of the importance of accurate information and public interest media coverage. Unfortunately, it also exposed just how unsustainable and fragile media industries have become in recent years as a result of the Internet’s disruption. For example, in the United Kingdom “the problem for commercial [TV] channels is that there are very few advertisements to show to these enlarged audiences [resulting from people being stuck at home during the lockdown], as companies cut their marketing budgets ahead of the impending recession. One insider at a commercial channel said British TV advertising is down 40% for the three months between March and June.” Similar impact is expected in the newspaper industry, with commentators stating that “thousands of journalists will lose their jobs.”<sup>8</sup> The impact of the crisis is likely

to be much greater in smaller markets and in developing countries, where media industries have already suffered greatly in recent years.<sup>9</sup>

Despite this disheartening context, two major developments took place in the first half of 2020 that give some hope to public interest media and to journalism’s business model.

### **First steps towards revenue sharing in Australia**

The first one is the decision by the Australian Competition and Consumer Commission (ACCC) to develop a framework to force Google and Facebook, which take the lion’s share of Australia’s USD 11 Billion<sup>10</sup> advertising market, to share advertising revenue with Australian media, which create a significant portion of the media content available online in that country. This decision came after a failed attempt to develop a voluntary code for tech companies to work with Australian media outlets in support of quality journalism.

“The mandatory code will have the same elements as the proposed voluntary code, but would also include penalties and binding dispute resolution mechanisms for negotiations between the digital platforms and news businesses. It will also define news content that would be covered by the code, and will encompass services beyond Google search and Facebook’s main platform, such as Instagram and Twitter...”<sup>11</sup>

The Australian model, which will be finalized in the second half of 2020, will provide a valuable set of best practices to other governments interested in regulating tech companies to encourage the sharing of advertising revenue in order to support public interest media. It will also yield valuable insights about the real ability and willingness of states to take on tech companies in order to advance the public’s interest.

Against this backdrop, perhaps it is time for the Internet Governance community to devote more energy to addressing some of these issues.

These may include, among other things, working towards the development of mechanisms for ad revenue sharing or investing in Artificial Intelligence (AI) technologies that optimize the visibility of credible sources of news sources, thus reinvigorating media outlets whose work contributes to the public good.

### An international fund for public interest media?

The second development is the release of a feasibility study, developed by BBC Media Trust, into the possibility of establishing an International Fund for Public Interest Media. The idea is that this fund would be financed by international development agencies, tech companies, and the philanthropic community, and that public interest media from the Global South or in contexts where freedom of expression is at risk would be prioritized for funding. In the words of one commentator:

“The prospects for achieving the Sustainable Development Goals without informed and engaged societies are remote. An independent public interest media system is critical to democratic self-determination and to economic development... The mission of the International Fund for Public Interest Media will be to support the development, sustainability and independence of public interest media especially in resource poor and fragile settings. Public interest media is defined here as media that is free and independent, that exists to inform publics on the issues that shape their lives in ways which serve the public’s rather than any political, commercial or factional interest, to enable public debate and dialogue across society, and to hold those in power to account on behalf of the public interest.”<sup>12</sup>

The feasibility study explores several models to guarantee transparency and impact and envisions seed funding of 100 million USD coming from different sources, though its long-

term objective would be to manage as much as one billion USD per year. Support would focus on national and local level media, investigative journalism, and regional and international media, and would be managed from four regional offices in Africa, Asia, the Middle East, and Latin America & Caribbean.

It remains to be seen how potential donors react to this idea, and it’s also not clear whether a centralized fund of this nature would really be the best way forward. It’s also not clear how or whether the fund would go about supporting non-commercial media, such as community radio networks, which often serve low income communities and usually struggle with financial sustainability. Nevertheless, the publication of this study reflects a growing understanding among development policymakers about the critical role that media and information play in the advancement of democracy and inclusive development.

While these two developments are still months or even years away from having a tangible impact on public interest media, they are certainly quite encouraging, especially at a time when the foundations of liberal democracy, which of course include the notion of a free and independent press, are being challenged.

For communication rights advocates and other actors interested in the viability of public interest media, the first step of this process should be to agree on key principles to guide these efforts, which should necessarily include the notion that media viability will need accountable and transparent mechanisms that prioritize democracy and human rights. ■

#### Notes

1. American Civil Liberties Union (ACLU). Freedom of the Press. <https://www.aclu.org/issues/free-speech/freedom-of-the-press>
2. UNESCO (2008). Media Development Indicators. International Programme for the Development of Communication. <https://en.unesco.org/programme/ipdc/initiatives/mdis>
3. Diamond, Larry (2010). “Liberation Technology” in Journal of Democracy, July 2010, Volume 21, Number 3. <https://www.journalofdemocracy.org/articles/liberation-technology/>
4. Mounk, Yascha (2018). “Can Liberal Democracy Survive Social Media” in The New York Review of Books. <https://www.nybooks.com/daily/2018/04/30/can-liberal-democracy-survive-social-media/>

5. Oghia, Michael J. Governing Digital Convergence: An Issue Paper on Media Development and Internet Governance. Global Forum for Media Development. <https://gfmd.info/internet-governance/>
6. Oghia, Michael J. Governing Digital Convergence: An Issue Paper on Media Development and Internet Governance. Global Forum for Media Development. <https://gfmd.info/internet-governance/>
7. Freedom House (2019). Freedom in the World in 2019. <https://freedomhouse.org/report/freedom-world/freedom-world-2019/democracy-in-retreat>
8. <https://www.theguardian.com/media/2020/apr/17/how-covid-19-turned-the-uk-news-and-entertainment-industry-upside-down>
9. <https://www.japantimes.co.jp/opinion/2020/05/04/commentary/world-commentary/local-news-covid-19/#.XrxDtGhKjcc>
10. <https://www.thedrum.com/news/2019/07/12/australian-advertising-spend-reach-23-billion-2023>
11. <https://www.theguardian.com/media/2020/apr/19/facebook-and-google-to-be-forced-to-share-advertising-revenue-with-australian-media-companies>
12. <http://downloads.bbc.co.uk/mediaaction/pdf/policybriefing/feasibility-study-ifpim-april2020-executive-summary.pdf>

Lorenzo Vargas is a communication for development specialist and researcher on citizens' media. He coordinates the Communication for Social Change programme of the World Association for Christian Communication (WACC), supporting community media initiatives in Asia, Latin America, the Caribbean, the Pacific, and Africa. He holds a Hons. BA in Development Studies from York University, an MA in Communication from McGill University, and has pursued further studies on media research and policy at the University of Brasilia and the University of Oxford. His publications include *Expanding Shrinking Communication Spaces* (co-editor) (Southbound, Penang, 2020).

# Tensions between media censorship and regulation in Jamaica

**Brittany Forsythe**

*Media regulation according to Fredman (2015) is defined as the process by which a range of specific, often legally binding, tools are applied to media systems and institutions to achieve established policy goals such as pluralism, diversity, competition, and freedom. Regulation consists of the deployment of formal statutory rules laid down by public authorities as well as more informal codes of conduct developed and implemented by media organizations in conjunction with the state.*

In essence, the media are regulated or controlled in such a way as to enable diversity, to provide access to opinions and are supervised by an authority. Anastaplo (n.d) posited that censorship is the changing, suppression, or prohibition of speech or writing that is deemed subversive of the common good. In media, regulation involves the suppression of speech or any information that may be seen as harmful, sensitive, offensive, or morally distasteful.

The similarity between both words relies on there being established guidelines or codes that are expected to be followed by media entities. However, no matter how thin the writer still believes that there are strong differences between the two terminologies which create distinctions. These variations create a palpable tension between censorship and regulations as it relates to broadcast laws due to the differences between the two terms based on the degree of stringency, morality,

and suppression that each concept embodies.

In Jamaica, the Broadcasting Commission is the regulatory body established to control media in the country. The commission was established as an independent body in 1986. The Commission outlines its main purpose as to serve as a regulator that leads and facilitates the development and advancement of a dynamic electronic communication sector for the benefit of Jamaica and the Caribbean. The Commission is mandated by the Broadcasting and Radio Re-diffusion Act (BRRA) to monitor and regulate free-to-air television, broadcast radio, and subscriber television (cable) services to ensure their operation at appropriate levels concerning technical, programming, and service standards.

Broadcast laws are implemented in two categories in Jamaica: The Broadcasting and Radio Re-diffusion Amendment Act and the Television and Sound Broadcasting Regulations. Broadcast laws are established and media entities are expected to follow the regulations outlined. Not following them could lead to sanctions and penalties.

### **Issues around freedom of expression**

Censorship is the suppression of expression and speech of a community or individual. Regulations, on the other hand, are guidelines established to ensure that wholesome and quality content is made available to citizens. According to the Jamaican Constitution, freedom of expression is a fundamental human right. Through censorship, in Jamaica, the Broadcasting Commission has laws that forbid the showing of certain films on television because of their content.

The movie “Amistad”, released in 1997 and directed by Steven Spielberg, had an opening scene in Jamaica that discussed slavery. Slavery is an important part of Jamaica’s past and it is a memory that many Jamaicans share. The relevant authorities, however, felt that the scene of a slave ship revolt was inappropriate for Jamaican audiences. Such censorship is an outright infringement of human rights as it seeks to conceal the beliefs and expressions of the people.

Censorship acts as a tool of control to conceal historical beliefs and by extension to silence the public. Regulations, however, have specific guidelines that control what is shown at what time. Therefore, it is not a complete ban, but there are codes and directives outlined. Under the Children’s Code for Programming, for example, the programme is evaluated, and licensed media are required to rate, schedule and issue advisories in relation to ratings which state the age group for the show such as PG 13 or PG 16. Television is also regulated to show adult programming in an encrypted manner between the hours of 11 pm and 4 am. Such content is aired during these times as it is assumed that most children would be asleep.

Tension is created as censorship is seen as imposing on fundamental human rights like access to information and to a larger extent the right to express oneself. It is therefore oppressive. While regulation is more of a rule book or code implemented to set a framework. The tension is highlighted in the nature of the two. Censorship allows for complete blocks and removals, while regulations establish a specific timeframe in which to show certain content, thus highlighting that censorship is more suppressive than regulation. This suppressive nature leads to tension with broadcast laws and it imposes the extent to which certain programmes may be aired.

Another clear difference that further creates tension is seen in that regulations are requests from the government along with the Broadcasting Commission to the people gracefully and politely not to do something in particular. On the other hand, censorship is harsher as the government or the authorities feel that if the material is not prohibited it could cause harm to the entire country. Government and authorities believe that if these materials or content go uncensored it could be detrimental to the common good, because it may be viewed as distasteful and offensive.

In communist nations such as Cuba, Ravnberg (2015) stated that there is the prohibiting of private ownership of the media and a declara-

tion which states that media may only be controlled by the State or society. In Cuba, media are highly censored and content from the United States is completely blocked as the Cuban government believes that if this culture is infiltrated into theirs it could cause mass damage for the people, ultimately leading to cultural imperialism and opposing paradigms.

The government has complete control over what is disseminated to the population and therefore curtails the content to align with the country's ideologies. In a democratic society such as Jamaica, stiff censorship measures are not in place to block all television programmes from a particular country. However, media regulations are established according to Lumen (n.d) to ensure equal airtime in the media, fairness in the media and the avoidance of defamation. Tension is further evident in the extent to which the two concepts are different. Both terms have different stringency levels as censorship leads to complete eradication or blocking of various content based on one's country; regulations, on the other hand, are more guidelines and measures employed to ensure quality and fairness in the media.

### Ethics lead to moderation

Ahluwalia (2011) posits another clear difference. Regulations are based on ethics, making regulation a synonym for moderation. They act as a code of conduct in society, keeping certain content within limitations. Regulations would, therefore, include the use of frequencies assigned to a radio station and media entities having to be licensed before coming on air. Censorship, on the other hand, is much harsher in nature as it is based on morals and involves specific "Do's and Don'ts" that must be followed through by agencies.

Esther (2009) states that dancehall and its actors behave in such a way that cannot be ignored as it disrupts moral standards and poisons children. In Jamaica, our culture of dancehall music has been censored by the Broadcasting Commission. Hopeton Dunn, chairperson of the Commission, postulated in a JIS article that

there shall not be transmitted through radio or television cable services, any recording, live song or music video, which promotes the act of "daggering" or which makes reference to, or is otherwise suggestive of, "daggering".

The Commission rules that these "daggering" lyrics outrightly contradict provisions in their regulations, specifically 30(d) and 30(l) which state respectively "No licensee shall permit to be transmitted d) any indecent or profane matter, so, however, that any broadcast to which regulation 26 relates shall be deemed not to be indecent; Reg. 30(d) (l) any portrayal of violence which offends against good taste, decency, or public morality. Reg. 30(l) (*The television and sound broadcasting regulations, 1996*).

In February 2009, a directive was given by the Broadcasting Commission of Jamaica, severely censoring the popular hit by Vybz Kartel and Spice known as "Ramping Shop". The song was filled with sexual lyrics classified under the daggering sub-genre of dancehall music. The song, which was laced with sexually explicit content, resulted in the entire censorship of the daggering sub-genre by the Broadcasting Commission of Jamaica. This shows the degree to which censorship relies heavily on morals thus causing it to be harsher.

Many Jamaicans are of the opinion that dancehall music has fostered a decay in public morals, and therefore censoring it would lead to an improvement. However, morals are often relative and dependent on the person, therefore making general rules based on morals creates tension as outrageous and offensive to one group may be the norm and appropriate to another group. Regulations seek to maintain order and cohesiveness, but censorship imposes on the rights of a journalist to showcase content and information to the public.

From this discussion it is clear that even though both concepts seem similar there are clear distinctions. It is upon this premise that a palpable tension can be noted between censorship and regulation as it relates to broadcast laws. Based on the research conducted and evidence

shown it can be concluded that censorship infringes on human rights while regulations are guidelines of control. Censorship is harsher depending on one's country, while regulations tend to promote equality and fairness. Lastly, censorship relies heavily upon morals contrary to regulations that rely on ethics. These differences play a vital role in the palpable tension seen between regulations and censorship as it relates to broadcast laws. ■

## References

- Ahluwalia, P. (2011). The Fine Line Between Censorship and Regulation in Social Media. Retrieved from <https://www.business2community.com/social-media/the-fine-line-between-censorship-and-regulation-in-social-media-0104445>
- Anastaplo, G. (n.d.). Britannica Dictionary-Censorship. Retrieved from <https://www.britannica.com/topic/censorship>
- Broadcasting Commission. (2014). Organizational Overview. Retrieved from <https://www.broadcastingcommission.org/about-us/organisation-overview>
- Broadcasting and Radio Re-Diffusion Act Jamaica. (2008). Retrieved from <https://moj.gov.jm/laws/broadcasting-and-radio-re-diffusion-act>
- Constitution of Jamaica. (1962). Retrieved from <https://www.refworld.org/docid/3ae6b4ed28.html>
- Esther, T. (2009.) 'Rampin' Shop' – Musical Poison. *The Gleaner*, Commentary.
- Freedman, D. (2008). *The politics of media policy*. Cambridge, UK: Polity.
- Jamaica Information Service. (2009). Broadcasting Commission Moves Against 'Daggering' Music on Radio and TV. Retrieved from <https://jis.gov.jm/broadcasting-commission-moves-against-daggering-music-on-radio-and-tv/>
- Lumen. (n.d.). Media: How they are regulated. Retrieved from <https://courses.lumenlearning.com/american-government/chapter/regulating-the-media/>
- Ravberg, F. (2015). Havanah Times- Cuban Press Law. Retrieved from <https://havanatimes.org/opinion/cubas-press-law/>
- Television and Sound Broadcasting Regulations Jamaica. (1996). Retrieved from [https://www.broadcastingcommission.org/images/TV\\_Sound\\_Broadcasting\\_Regs.pdf](https://www.broadcastingcommission.org/images/TV_Sound_Broadcasting_Regs.pdf)

Brittany Hutchinson is reading for the Bachelor of Arts degree in Journalism at the University of the West Indies, Mona, Kingston, Jamaica.

# IAMCR anti-racism statements

*The International Association for Media and Communication Research (IAMCR)'s Clearinghouse on Public Statements and its Executive Board issued two statements in June 2020 related to the anti-racism protests taking place in the United States and elsewhere. The Clearinghouse statement is in support of the right of journalists and news outlets in the United States to observe and report events freely and safely, while the Executive Board Statement is in solidarity with all those who insist that Black Lives Matter, who demand an end to all institutional practices that deny equality, dignity and opportunity, and who call for a resolute commitment to the renewed pursuit of economic, social and cultural justice.*

## Statement on Journalist's Rights in US Protests

IAMCR supports the right of journalists and news outlets in the United States, covering the unfolding protests against widespread patterns of state violence directed at black and brown Americans, to observe and report events freely and safely. The deliberate targeting, by law enforcement officers, of journalists doing their jobs is a direct assault on the principles of freedom of speech and of the press guaranteed both by the First Amendment of the United States Constitution and Article 19 of the Universal Declaration of Human Rights.

As of June 6, 2020, the U.S. Press Freedom Tracker, an online database created by the Com-

mittee to Protect Journalists and the Freedom of the Press Foundation, has identified 173 separate incidents across the country where journalists, including student journalists, were arrested, physically attacked, tear gassed, pepper sprayed, shot with rubber bullets or targeted with stun grenades by U.S. law enforcement officers.

Numerous U.S. news sources reported that the President of the United States recently deployed U.S. Park Police and armed military personnel to disperse a peaceful demonstration on U.S. soil so that he could be photographed holding a Christian bible in front of a church. Among those who were assaulted were journalists documenting the event. This is inconsistent with the right to public assembly and protest to give voice to the desire for change.

IAMCR calls on police chiefs, mayors and governors in the United States to ensure that journalists can cover events comprehensively, including public instances of indiscriminate police violence against protesters. It is essential for them to be able to provide the vital evidential base for a fuller understanding of the underlying reasons for the protests.

*This text of this statement was drafted by the Clearinghouse for Public Statements and approved by Professor Janet Wasko, president of IAMCR. The Clearinghouse processes statements and/or manages the process of signing statements generated by others, that are principally concerned with issues relating to media/communications and where IAMCR members have substantive scientific expertise that provides a basis for seeking to influence discursive or material practice.*

## **Black Lives Matter**

The brutal and wilful killing of a middle-aged black man, George Floyd, on May 20th in Minneapolis by a white police officer, who knelt on his neck while arresting him for supposedly possessing a counterfeit bank note, has detonated global demonstrations. Around the world people have gathered to protest the endemic racism of law enforcement agencies and dominant insti-

tutions and confront the unresolved legacies of slavery and colonialism that sustain black and ethnic minority peoples' continuing experience of everyday discrimination and dismissal.

The protests have erupted globally. In Bristol, UK the statue of the slave trader Edward Colston has been torn down and thrown into the harbour. In Australia, crowds have chanted 'I can't breathe' – the last words of both George Floyd and David Dungay, a young aboriginal man who died in custody in a Sydney jail in November 2015. And everywhere people have knelt for the eight minutes and forty-six seconds it took George Floyd to die.

As a scholarly community with members from over ninety countries, the International Association for Media and Communication Research ([IAMCR](#)) stands in solidarity with all those who insist that Black Lives Matter, who demand an end to all institutional practices that deny equality, dignity and opportunity, and who call for a resolute commitment to the renewed pursuit of economic, social and cultural justice. ■

*Made available under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 License.*

## ON THE SCREEN

### Nyon (Switzerland) 2020

At the 51st Festival Visions du réel Nyon (April 17 – May 2, 2020), the interreligious watched and discussed the 14 films of the competition for long films due the Covid-19 situation online and awarded its Prize of CHF 5'000, donated by the Swiss Catholic Church, the Reformed Churches in the French-speaking part Switzerland (CER) and its Media Department Média-pro, and the Swiss Federation of Jewish Communities, to the film *Off the Road / Fuera del camino* directed by von José Permar (Mexico/USA 2020).

*Motivation:* The director takes a head on approach, sometimes with the skill of a racing driver, to tackling all the issues faced by changing societies: the roots that define the identities of people and communities, the relationships between generations as well as men and women, the different social, economic and political categories, and the desert environment of Mexico's Baja California, which plays host every year to a car race watched by thousands of fans. All of which is treated with humour and music for a project that will involve even more petrol heads.

### Oberhausen (Germany) 2020

At the 66th International Short Film Days Oberhausen (13-18 May 2020) the Ecumenical Jury appointed by INTERFILM and SIGNIS awarded its Prize of € 1500, donated by the Catholic Film Work and the Protestant Church of Oberhausen, to *Shepherds* directed by Teboho Edkins (France, South Africa, Germany, 2020).

*Motivation:* The film shows the psychological drama of shepherds from Lesotho, some of whom were sentenced to nine years in prison for having stolen cows. This film caught the

attention of the Ecumenical Jury for the originality of the theme, the love of a community of Lesotho for cows, for professionalism in photography direction and image aesthetics, the silences which invite the spectator to meditation.

The film shows the value of cows in the lives of members of this community. But it also draws public attention to the gap between the wrongdoing and the punishment.

In addition, the jury awarded a Commendation to *Las muertes de Arístides / The Many Deaths of Arístides* directed by Lázaro Lemus (Cuba, 2019).

*Motivation:* For the innovative, original and intimate approach to the subject of war, life and death. The animation of a silhouetted figure, journeying on a boat through the dark fuses with the frozen moments of time as we hear the letter of a young man that never returned home. His prayer for Olga centralises the film as hope, as a cry to God for the life of the other, as love outshining the depths of darkness. The film makes memory alive and breaks the time boundaries, transcending visually what cannot be described in words, and as such it is a work of pure cinema.

The jury awarded a second Commendation to *Milenina píseň / Milena's Song* directed by Marie Lukáčová and Anna Remešová (Czech Republic, 2019).

*Motivation:* The creators of *Milena's Song* reveal the theme of core spirituality in their movie. They depict a story of a cleaning lady who finds her own way of manifestation of faith while being in the shadow of institutional hierarchy. Her original prayer dance opens for the viewers her initial nature of believer referring to times of the early church fathers and reminding of cultural decentralization and non-hierarchical nature.

Furthermore, the Ecumenical Jury attributed Recommendations for two films in the Youth Film Competition: *Warum Schnecken keine Beine haben / Why Slugs Have No Legs* directed by Aline Höchli (Switzerland, 2019) and *I'm Not Your F\*\*\*ing Stereotype* directed by Hesome Chemamah (Thailand, 2019). ■