

To cite this article:

Calzada, I. (2019), Data Spaces and Democracy, *RSA Journal*. Issue 2: 40-43.
[DOI: 10.13140/RG.2.2.35392/89601/1](https://doi.org/10.13140/RG.2.2.35392/89601/1).

Data Spaces and Democracy

*As our cities become increasingly smart,
are we able to ensure that they remain democratic?*

By **Dr Igor Calzada, MBA, FeRSA**

www.igorcalzada.com/publications

igor.calzada@compas.ox.ac.uk

@icalzada

Dr Igor Calzada is a research fellow, policy adviser and lecturer at the University of Oxford Urban Transformations ESRC and Future Cities programmes

“We are already becoming tiny chips inside a giant system that nobody really understands”. So wrote Israeli historian Noah Yuval Harari about our current experience of urban living, which, increasingly, is mediated by AI. AI is now an important component of sectors such as healthcare, agriculture, public administration and transportation, and is helping to address major challenges such as ageing and climate change. However, there is currently a lack of transparency in algorithmic governance systems, and this is worsened when these algorithms are integrated into already opaque governance structures in our cities. Moreover, over the past decade, the propagation of sensors and data collection machines in so-called ‘smart cities’ by both the public and the private sectors has created democratic challenges around AI, surveillance capitalism, and protecting citizens’ digital rights to privacy and ownership.

In 2018, the General Data Protection Regulation (GDPR) came into force in the EU. This regulation harmonised data privacy laws across Europe and is aimed at protecting citizens’ data and giving people control over their own data. Against this backdrop, a debate has emerged in European cities and regions about the role of citizens in their cities and how they control and understand their own data.

Data ecosystems are the infrastructure, institutions, analytics and data capture systems that are used to take data and relay it to the system owners, who can then alter their provision of goods and services and marketing accordingly. Little is known about the long-term socio-political effects of these systems, which we are increasingly reliant on. The present momentum around privacy concerns could be seen as a call to action to create democratic digital infrastructures and institutions in Europe. The public sector needs to innovate and to involve a plurality of stakeholders. More radically, the ownership of platforms – currently predominantly in the hands of private companies – as well as data itself could be *co-operativised*. Such an approach in Europe would trailblaze citizens’ digital rights protection and avoid algorithmic extractivism and surveillance.

If we allow data ecosystems and AI to develop with insufficient oversight, algorithmic disruption will have consequences in a wide range of areas, including employment, income and gender equality, privacy, bias, access, machine ethics, weaponisation, social capital and service provision. According to Cisco ISBG, by 2020 facial recognition and individual

profiling will be driven through 50 billion connected devices, all feeding data to AI platforms. In theory, this could make our experiences of cities far more tailored and effective as our data are used to provide the most needed services and pinpoint areas where cities are underperforming. The idea is that AI could make better decisions than humans. AI gets smarter the more data it is fed, but it also learns human and societal biases, thereby creating the conditions where the most vulnerable social groups are marginalised further. For example, the Microsoft chatbot was taught racist phrases by Twitter users. The American political scientist Virginia Eubanks' work shows how the poorest and most in need sections of society are those who are under the most surveillance by automated systems, which can often make mistakes.

If it is to address some of these risks and increase public benefit, governments and the public sector needs to embrace AI; unless they take more responsibility for the handling of citizens' data, for-profit companies will dominate the techno-deterministic smart cities agenda. Local and regional authorities need to show citizens that they will protect their data and rights, and that data will be used in responsible ways. Once this trust is established, people may be in turn more willing to agree to the use of AI in various government services.

The European Commission is leading the way in this field. It is developing an expanded network of digital innovation hubs, which could be central to the development of local and regional 'data policy ecosystems', bringing AI training, data, computing and local partnerships together to develop AI solutions that are adapted to local and regional issues.

Digital rights in smart cities

Over the past ten years, working collaboratively on smart cities and the techno-politics of data with local and regional authorities, firms, academics, non-governmental organisations, and (social) entrepreneurs and activists, under several policy and research schemes, I have concluded that the smart city has been built on hubris and the false assumption that just being digitally connected or plugged in means being *smart*. The advocates of smart cities wrongly still think that real-time data flows can be used to optimise cities' central nervous systems through 'digital twins' (virtual models of real-world processes, products or services) without any democratic cost. They promise big improvements in energy savings, mobility and transport efficiency, replication capacity and sustainable land use. Yet many smart city experiments demonstrate the shortcomings of this point of view.

Valuable lessons about how not to build smart cities from scratch can be drawn from Songdo in South Korea, Masdar in Abu Dhabi (both of which were designed to be smart, eco-friendly cities, but which remain ghost towns) and even Toronto in Canada. The Google/Alphabet Sidewalk Labs flagship project in Toronto has triggered a fierce backlash, with Google accused of infringing citizens' digital rights and thus subverting democracy. Critics are concerned that questions about who owns the data collected by Sidewalk Labs 'digital layer' are not being adequately addressed.

In contrast, since 2015, Barcelona has been pursuing the explicit protection of digital rights through technological sovereignty by emphasising grassroots-led urban experimentation, data commons (platforms where data is considered part of the public infrastructure, or a common asset, and is stored and shared under set principles) and public return. How the Toronto and Barcelona experimental approaches fare in the coming years will inform policymakers around the world.

The demise of democracy is clearly already one of the biggest policy challenges of our time, and the undermining of citizens' digital rights is part of this issue. These include a wide range

of complex rights that need to be addressed alongside legal and human rights in a digital world. They include the right to be forgotten on the internet, the right to be unplugged or disconnected, the right to your own digital legacy, the right for your personal integrity to be protected from technology, freedom of speech online, the right to your own digital identity, the right to the transparent and responsible use of algorithms, the right to have a last human instance in expert-based decision-making processes, the right to equal opportunities in the digital economy, consumer rights in e-commerce, the right to hold intellectual property on the internet, universal access to the internet, the right to digital literacy, the right to impartiality on the internet and the right to a secure internet.

So how will AI affect cities and, more directly, citizens' digital rights? How can cities control their technologies, infrastructure, and provision of services while utilising data in a democratic, citizen-led fashion?

Post-GDPR AI

GDPR is perhaps the first time that the EU has taken the initiative in digital matters and spoken with its own voice, blending data and smart city research and policy formulations. From here onwards, new data policy ecosystems are needed to consolidate a strategy for the protection of citizens' digital rights across Europe. This should entail a call to action, a need to critically map out the techno-political debate on *dataism* and, ultimately, it should identify the potential requirements to establish regulatory frameworks to protect digital rights. It is crucial to understand how the concepts of autonomy and identity of individuals, as well as security, safety, privacy, and ownership might change under the influence of AI. To build and retain trust in AI and the use of citizens' data requires critical engagement of civil society.

One direct outcome of GDPR is the Cities Coalition for Digital Rights (CCDR) movement. This broad movement already encompasses 30 international cities and has the support of the UN-HABITAT programme. Under the leadership of Barcelona and the joint strategic view of Amsterdam and New York, the network is being extended further. CCDR plans to address two main policy challenges in the short term to better react to the consequences of AI for citizens.

The first policy challenge is to gradually replace the centralised and extractive 'platform-knows-best' capitalist model of the smart city that has taken over many cities. This should be done by enacting sectoral policies in conjunction with experiment-driven 'platform co-operatives'. A platform co-operative is a co-operatively owned, democratically governed business model that establishes a computing platform and uses a website and/or mobile app to facilitate the sale of goods and delivery of services. For example: Fairbnb, a vacation rental platform, gives 50% of its revenue to local community projects; Denver's Green Taxi Cooperative, which is owned by its workers; and Resonate, a streaming music service that shares profits with various stakeholders.

In Barcelona, three projects on participatory democracy have set the scene for a transition towards platform co-operativism: DECODE, which provides the tools for individuals to be in control of their personal data; Decidim, which helps people, organisations and governments to self-organise in a democratic way; and Metadecidim, the democratic community that manages Decidim projects. Platform co-operatives require a strong alliance between institutional capacity, active civic society, and entrepreneurial business ecosystems. They are social and ethical alternatives to existing commercial extractivist platforms.

The second policy challenge is how to consolidate a pan-European post-GDPR AI through 'data co-operatives'. These enable the creation of open data and personal data stores for mutual

benefit. The unbridled extractivism of personal data by big tech private ‘data-opolies’ needs to be stopped. Local and regional authorities should establish data co-operatives in order to empower citizens to have more control over their data and give them more of a say in the services that are built on and informed by this data. This may help to rebalance the relationship between those who create data (citizens) and those who seek to exploit that data, while also creating the environment for fair and democratic exchange.

Data co-operatives with fiduciary obligations to members demonstrate a promising direction for the democratic empowerment of citizens through their personal data. Without data co-operatives and their related data policy ecosystem, the EU might lose its opportunity to establish a pan-European post-GDPR AI strategy. Unlike in China or the US – the data governance paradigms of which are driven by either the state or big tech corporations respectively – the debate around data in the EU is currently open, and the EU has the opportunity to lead in this area. City and regional authorities must collaborate further on the ethical and social benefits of data capture and AI for their citizens.

Could an ecosystem of data co-operatives in Europe protect citizens’ digital rights and better tailor the design, implementation, and assessment of further citizen-centric AI? To ensure European cities and regions employ data democratically, the public sector should take the lead alongside various stakeholders. Debating the techno-politics of data for citizens is not just ethic washing; it should be about ownership and how to rescue democracy. Failing to do so could risk exposing European democracies to the stealthy algorithmic manipulation of collective behaviours through social media, resulting in a dystopian populism.
