THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

RESEARCH FOR THE WORLD

An equitable society depends on holding Big Computing firms to account

Published 9 November 2021

Dr Seeta Peña Gangadharan is Associate Professor in the Department of Media and Communications at LSE. Her work focuses on inclusion, exclusion and marginalisation, as well as questions around democracy, social justice and technological governance.

What might advances in AI and computing mean for marginalised communities who already face discrimination in both the material and virtual worlds? **Seeta Peña Gangadharan** explores the impact of Big Computing ambitions on freedom and control.

Questions of bias in artificial intelligence are all the rage. Researchers and practitioners worry about encoding racism, sexism, and other problems into automated decision making and seek technical solutions for "fairness". But this framing of contemporary tech problems focuses too much on the technology itself, neglecting the deeper interventions required to address issues of freedom, control, and Big Computing.

You will have heard of Big Data, but Big Computing refers to the ever-expanding ecosystem of institutions and processes needed to operate, maintain, and grow automated services. It depends on well-resourced companies, like Google or Amazon, who sit atop the pyramid for data-driven services. In explaining this ecosystem – or computational infrastructure, as they call it – computer scientists Gürses, Troncoso (**Privacy Engineering Meets Software Engineering. On the Challenges of Engineering Privacy By Design, 2020**) and others describe automated services as involving several different layers of computational processes, whose coordination benefits from an institution that centralises coordination between the layers.

As the mention of Google and Amazon should suggest, there is an overlap between Big Computing and Big Tech. Both want to expand their reach. Both have few competitors. But big computational service providers are nearly impossible to avoid for any institution looking to optimise and automate: whether assisting an institution in managing operations, resources, client relations, service delivery, or more, the bottom line is *computational service providers integrate themselves into the very DNA of these institutions.* While these organisations might also benefit from the publicity that Big Tech platforms afford them, without Big Computing services, business operations would cease altogether. In this sense, if data is so-called the "new oil," then computational infrastructure is the "new oxygen."

> As Big Computing consolidates power into the hands of a few larger companies… groups who live at the intersection of myriad systems of oppression increasingly face new burdens and new barriers.

New tech solutions could increase the marginalisation of certain communities

In my work on technology and marginalisation, the rise of Big Computing and its oxygenic enterprise is critically important to unpick.

As Big Computing consolidates power into the hands of a few larger companies who determine the fundamental operations of public and private institutions, individuals and groups who live at the intersection of myriad systems of oppression increasingly face new burdens and new barriers.

Members of marginalised groups already deal with opaque public or private institutions that are meant to serve them whilst often punishing or exploiting them. They must now tackle an opaque computational ecosystem as it goes about replacing institutions' core operational processes with so-called efficient and optimal automated services.

Coercive adoption is a feature, not a bug, of Big Computing. On-the-ground stories shared in the field reveal that people feel like they are forced to adopt tech solutions implemented by the public and private institutions which serve them. Whether in the context of public safety, health, shelter, employment, or caregiving, there can seem no option but to engage with automated services.

> At some point in the not-too-distant future, it is possible to imagine computational service providers claiming to be more 'intelligent' than the police in finding criminals and deterring crime, and so replacing police 'intelligence'.

We are already seeing technology fundamentally changing policing

In recent years, the European police (both domestic and border forces) have begun shifting their institutional practices and introducing police technologies.

Police tech ranges in sophistication. It can include relatively low-tech tools, like databases that catalogue suspected gang members or criminal offenders. It also includes high-tech tools that require greater computational power and sophisticated computational infrastructure. For example, police make use of drone policing, facial recognition, predictive policing, and other technologies that process and share large volumes of data in real time.

These technologies also range in ownership and control models. Some, like a criminal database, are developed and managed in-house. But other tools require outside vendors, who compete to offer attractive pricing packages for their data-driven products, including user-friendly analytic tools and free storage.

Police tech is transforming where policing takes place. "Smart" doorbell systems and privately implemented facial recognition cameras - and the computational infrastructure working in the background - can easily rival public networks of street cameras and the analysis of CCTV data. At some point in the not-too-distant future, it is possible to imagine computational service providers claiming to be more "intelligent" than the police in finding criminals and deterring crime, and so replacing police "intelligence". In this scenario, the police would not be abolished. Instead, they and the protocols and procedures in place to keep them in check would be replaced by Big Computing.

> Whether intended or not, the fundamentally coercive nature of police tech aligns with [a] legacy of mistreatment.

Police tech extends discriminatory practices

This shift towards police tech is taking place in an institutional environment already deeply criticised for entrenched practices of racialised criminalisation. As documented by advocates, activists, and community members, police routinely profile members of black, Roma, and other minority communities, as well as those on the move (migrants, refugees and asylum seekers). In the UK, members of racialised communities regularly endure increased police presence, higher rates of stop and search and higher arrest rates. In the year before the pandemic, for example, black people were nearly ten times more likely than white counterparts to be stopped and searched. During the pandemic, the problem expanded. In London alone, black people accounted for nearly a third of lockdown arrests, despite being about 20 per cent of the population.

Outside of the UK, racialised criminalisation systematically appears in similar contexts. Minoritised communities were subject to pervasive targeting during mandatory lockdowns throughout Europe. In Serbia, quarantining of residents of Roma settlements and of people on the move was managed by the military. When the government lifted lockdown restrictions, freedom of movement remained restricted for those living in refugee and migrant centres.

Whether intended or not, the fundamentally coercive nature of police tech aligns with this legacy of mistreatment. Both low-tech and high-tech police tech make it easier to extend existing practices of profiling. They help law enforcement target so-called nuisance populations. They contribute to an overarching narrative that black people, people of colour, people on the move, and Roma are fundamentally dangerous and deserve to be watched. Moreover, by virtue of their technical design and computational operations, they are opaque and complicate efforts to demonstrate patterns of unfairness and injustice.

> As computational service providers grow more powerful... the public loses capacity to adequately and effectively contest the ways in which their public services are run.

Big Computing threatens not just marginalised communities but democracy itself

The case of police tech, its impacts on racialised communities, and the convergence between coercive police tech and the problem of racialised criminalisation point to a much larger, (eco)system-wide problem. If computational infrastructure is oxygen, public institutions are suffering from asphyxiation. Vendors target law enforcement (or any other public service, from health to transport to welfare services), offer services that outperform public ones, and help drive demand for computational services. As computational service providers grow more powerful, not only do public institutions diminish their ability to manage problems and evaluate impacts, the public loses capacity to adequately and effectively contest the ways in which their public services are run.

While many proponents in computer science and the self-defined tech industry push for solutions like auditing and cleaning datasets, or adapting the parameters of algorithmic models, the extent of the problem warrants a more visionary solution. When coercion serves as the starting point for people's interaction with so-called predictive, "smart," optimising technologies, we need to actively intervene in the rise of Big Computing. Abolishing certain tools, not tweaking their functionality, is one path. Designing exit strategies from contracts for data-driven services is another path. Strengthening public services that support otherwise policed and punished populations is yet another.

These are propositions worth taking seriously. They draw attention to the need for autonomy and independence. Big Computing might not like it. But democracy depends on it. ■