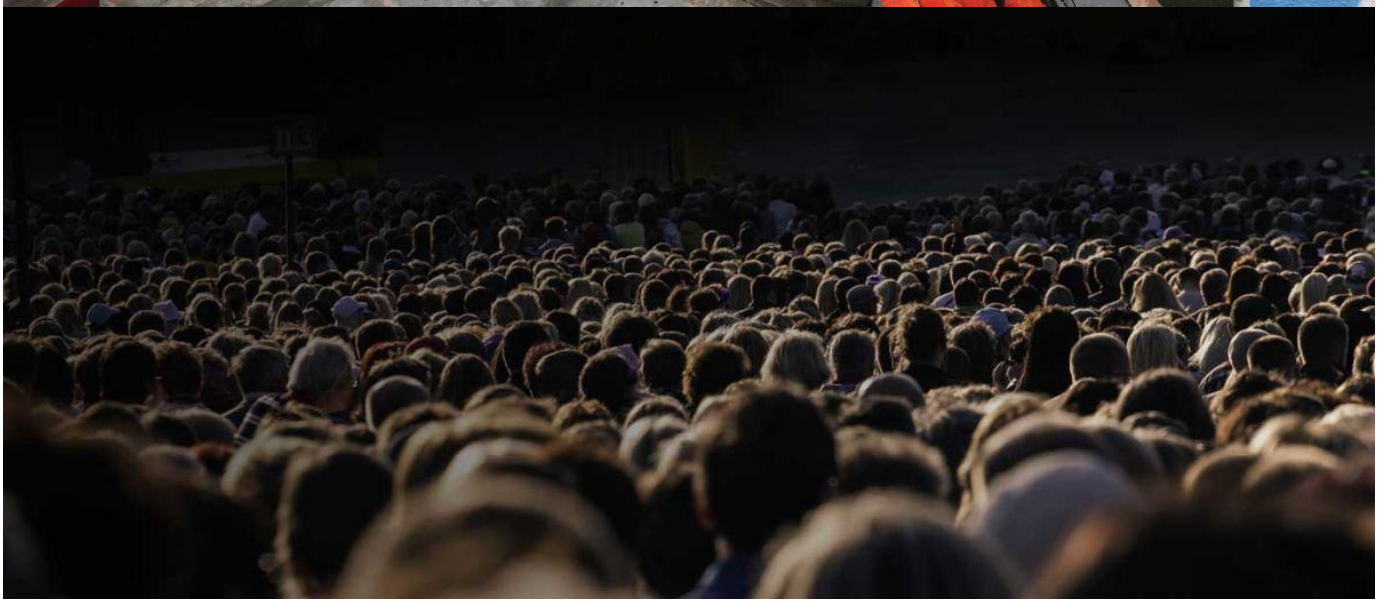

The Datified Globe: Emerging Trends in Algorithmic Governmentality

May 30, 2019 | Volume 12 | Issue 21
Brett Aho

Today, digital technologies and artificial intelligence (AI) are among the strongest forces shaping human societies. As the world becomes more digitally connected, more and more aspects of human life are mediated by technology. As a result, a broad global trend of datification is underway, translating more of everyday experience into digital text. And even though many are now familiar with the adage "data is the new oil," relatively few seem to actually grasp the implications of this emerging structural shift. Datafication is positioned to transform human societies in a manner unprecedented in human history.

This essay examines three emerging global trends in this transformation: surveillance capitalism, post-humanitarianism, and algorithmic authoritarianism. Each concept describes a nascent system of socio-economic organization made possible by processes of datification, improvements in AI algorithms, and the spread of a cybernetic epistemology that promotes practices of data-behaviorism (Rouvroy, 2012). *Surveillance capitalism* describes the power of big data as deployed by corporations operating under neoliberal logics (Zuboff 2019). *Post-humanitarianism* describes the extension of a data-focused cybernetic epistemology to practices of humanitarian intervention in the context of precarity and instability (Duffield, 2019). *Algorithmic authoritarianism* describes the use of big data and AI within governmental systems of social, economic, and political control (Feldstein, 2019).The first part of this essay will describe the technologies, theories, and epistemologies that underpin the function of each of these three trends. The second part of the essay will examine each system in turn.

Dataism as Ideology

Today, processes of "datafication" are rapidly transposing everyday life into data. With every transaction, every "like," click, swipe, tap of the finger and movement of the mouse, data is being collected, stored, and added to an expanding database of behavioral data that together creates an expanding profile of the individual.

Smartphones, home assistants, and other “smart” devices add to that repertoire, recording every utterance, conversation, and footstep. Emails, text messages and social media are scanned and analyzed; location and routine are tracked via mapping apps, GPS and bluetooth beacons; health and wellness data are recorded via DNA services, fitness devices, workout and menstruation apps; while mood and taste are recorded with every show watched and song listened to. When these data streams are put together, they create a fairly accurate digital representation of an individual's reality. With the application of AI to these data streams, humans become the subjects of algorithmic modeling; machines are thus able to “know” an individual in ways unavailable to that person themself.

Another way to understand the direction in which societies are rapidly progressing technologically is through the concept of “mirror worlds” as proposed by Yale computer scientist David Gelernter. The basic premise is that the real world will eventually become enmeshed with digital representations of that world, creating realities that are both digital and physical at once. Gelerneter (1991) describes mirror worlds as “software ensembles, glued-together out of many separate programs all chattering at once” (p. 8). As human behavior (interactions, relationships, decisions, movements, purchases, etc.) becomes increasingly modelled through expanding surveillance infrastructures, societies are witnessing the emergence of the mirror world in its infancy. Already these software ensembles are beginning to play a major role in societies around the world, driving corporate, government, and military decisionmaking processes.

With every transaction, every “like,” click, swipe, tap of the finger and movement of the mouse, data is being collected, stored, and added to an expanding database of behavioral data that together creates an expanding profile of the individual.

Cybernetics is at the heart of these developments. Essentially, human populations are treated as subjects of cybernetic control systems in which behavior is mediated through causal chains that move from action to analysis and comparison with desired goals, and again back to action, incorporating changes to improve effectiveness of action. As Duffield (2016) writes, “the global digital infrastructure now exists for cybernetics to shift from its former concern to make a machine equivalent of human cognition to now intervening within, practically shaping and remotely managing consumers, populations and environments globally as if they are

living automata” (p. 152). The consequences of this post-human cybernetic rationality is the erosion of qualitative, reality-based, interpersonal, reflexive thinking that previously underpinned most corporate and government decisionmaking processes prior to the computational turn.

Under systems of “algorithmic governmentality,” data streams processed by AI become the primary tools informing policy. While the data may allow for effective prediction, it does so by stripping individuals of their stories, their motivations, their emotions, and their agency. As a result, populations become distanced from their humanity, defined not by who they are, but by what data-processing algorithms say they are. The datified world implies a substantial ontological transformation of the ways that societies construct and interpret knowledge, as cybernetic epistemologies tend to devalue reason and critical thought in favour of observable and recordable behavior. Rouvroy (2016) refers to this increasingly ubiquitous ontology as one of “reliability without truth.”

Emerging Trends

The emergence and rapid rise of new surveillance infrastructures can be largely tied to neoliberal globalization and its dearth of regulatory oversight. The tech sector has very likely emerged as the least regulated industry in all human history relative to its size. As a result, tech corporations have marched further and deeper into the realms of data extraction and behavioral engineering. A 2017 TED talk by former Google design ethicist Tristan Harris describes “how a handful of tech companies control billions of minds every day.” Bi-directional data flows have resulted in biopower becoming increasingly embedded in new technologies, to the extent that those who are able to control technologies may also control populations.

Combined deployment of surveillance cameras, facial recognition technology, and AI in China. (Source: Reuters/Bobby Yip)

In liberal market economies, the US in particular, the development of big data and AI under neoliberalism has given rise to a powerful new mode of accumulation that Zuboff (2019) has termed surveillance capitalism. Karl Polanyi (1944) proposed that industrial market capitalism functions through the construction of three “fictional commodities” in which nature is reframed as real estate, human life is reframed as labor, and exchange is reframed as money. Zuboff (2019) proposes the emergence of a fourth fictional commodity in which reality is reframed as behavior. Tech companies in the US, including Google, Facebook, Amazon, and Verizon, have all premised their future growth on the development of a new business model which extracts data from individuals and applies AI algorithms in order to understand and manipulate customer behavior at the individual level. The same surveillance model has since spread throughout the economy, achieving prominence in the insurance, banking, automobile, and retail sectors.

In authoritarian contexts, states have begun to co-opt the surveillance capacities of new digital technologies for purposes of socio-economic control. China in particular has paved the way for the emergence and spread of a new governance style that has has been variously referred to as digital authoritarianism or algorithmic authoritarianism. China’s Social Credit System is perhaps the most prominent

example. In brief, the system assigns a series of dynamic algorithmically determined credit scores to all firms and individuals, rewarding those who exhibit desirable behaviors while punishing those who demonstrate undesirable behavior. The system is enabled by massive data-sharing agreements with tech, telecom, and financial industries, and is complemented by the world's largest network of facial-recognition CCTV cameras. The risks of algorithmic authoritarianism can be read in Xinjiang Province where Chinese tech companies are developing new AI-based surveillance systems that monitor minority Muslim populations and employ predictive policing systems that aim to identify security threats before they emerge (Human Rights Watch, 2019). As China seeks to market these new technologies beyond its borders, the world may soon witness a golden age of authoritarianism, characterized by the marriage of surveillance and AI (Feldstein 2019).

Bi-directional data flows have resulted in biopower becoming increasingly embedded in new technologies, to the extent that those who are able to control technologies may also control populations.

In the context of instability, where precarious populations are predominately serviced by the humanitarian sector, the logics of data-behaviorism have also emerged as the dominant method by which organizations now function and operate. The practices of NGO and humanitarian aid organizations have become increasingly rooted in a positivist epistemology, where metrics have come to replace critical and reflexive observation. Building off Hannah Arendt's concept of the "boomerang effect," Duffield (2018) argues that colonial practices of using precarious populations as political and economic testing grounds never really stopped, and that "the global South currently functions as an unregulated commercial laboratory for the development of smart technologies and data mining experimentation that would be politically difficult in the North" (p. 158). Further evidence of data-behaviorism can be found in the World Bank's attempt to apply the logics of behavioral economics to the development sector; the organization's publication *Mind, Society, and Behavior* is particularly illustrative in this regard (World Bank, 2015, p. 81).

Datafication is occurring at a rapid pace in societies around the world, with substantial implications for how corporations and governments function. In the US, surveillance capitalism has thus far progressed without substantial resistance; however as civil society begins to wake up to its implications, there are signs that policy changes may be on the horizon. Meanwhile, Europe has already embraced its

General Data Protection Regulation (GDPR), which can be interpreted as a substantial normative statement rejecting algorithmic governmentality; however this policy may also incur economic costs by restricting European companies' ability to develop new AI technologies. China, as we have seen, seems less concerned about data protections than technological leadership in surveillance infrastructures and data-behavioralist capacities designed to enhance socio-economic control. As these technologies continue to advance, societies around the world will find themselves facing important decisions about how to embrace, reject, or regulate new forms of algorithmic governmentality. In a datified world, policy processes must continue to be complemented by qualitative and critical reflections, particularly so as societies make decisions about how algorithmic epistemologies will shape human futures.

Notes

Feldstein, S. (2019). The Road to Digital Unfreedom: How Artificial Intelligence is Reshaping Repression. *Journal of Democracy*, *30*(1), 40-52.

Gelernter, D. (1993). *Mirror worlds: Or the day software puts the universe in a shoebox... How it will happen and what it will mean*. Oxford University Press.

Human Rights Watch (HRW). (2019). China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App. *Human Rights Watch*. Retrieved from https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance

Duffield, M. (2016). The resilience of the ruins: towards a critique of digital humanitarianism. *Resilience*, *4*(3), 147-165.

Duffield, M. (2018). *Post-humanitarianism: Governing Precarity in the Digital World*. John Wiley & Sons.

Polanyi, K. (1944). *The great transformation: The political and economic origins of our time*. Beacon press.

Rouvroy, A. (2012). The End(s) of Critique: Data-Behaviourism vs. Due-Process. In M. Hildebrandt & E. de Vries (eds.), *Privacy, Due Process and the Computational Turn. Philosophers of Law Meet Philosophers of Technology* (pp.143–68). Abington: Routledge.

Rouvroy, A. (2016). ‘Of data and men.’Fundamental rights and freedoms in a world of big data. In *Bureau of the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS 108]*.

World Bank. (2014). *World development report 2015: Mind, society, and behavior*. World Bank Publications.

Zuboff, S. (2018). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.

Tags

technology

surveillance

biopolitics

Brett Aho is a PhD candidate in the Department of Global Studies at the University of California, Santa Barbara.

View PDF