Toin University of Yokohama
Research Bulletin, No.44, June 2021

Articles

AI–Algorithm–Big Data, Predictive/Automated Criminal Justice, and Hyper Crime/Social Control:

'Surveillance Capitalism' after 'Singularity' and Prospects of Information Civilization

TAKEMURA Noriyoshi

(Received Date: March 13, 2021)

I. Introduction

Current real society is surprisingly resembling a dark society in the near future which scientific fictions frequently draw. In famous scientific fiction "Minority Report" a policeman, who works at 'department of crime prevention' in Washington D.C., arrests would-be criminals based on pre-crime logic.

Big data, predictive software, and risk assessment algorithms have already significantly shifted the criminal justice landscape. These seemingly handy pieces of technology have the capacity to expedite and streamline the work of criminal justice actors, but may do so at the expense of those entering or already entrenched in the justice system. We should maintain a healthy skepticism about the use of big data and algorithmic decision-making, which are only likely to grow more ubiquitous as we head forth into an increasingly technologized future.

With advancing current situation and AI and IT have developed in the future, after the 'singularity' comes, what will happen around human beings? We need develop a 'critical analysis of AI-Algorithm-Big Data using predictive/automated hyper crime control', facing the surveillance regime of state-company-citizen trinity, which advances under the slogan of 'security and safety' from super to hyper, and under which make possible all kinds of social control based on the principle surveillance society, 'big data'.

In this article, concerning a 'predictive/automated hyper crime/social control', following problems are cleared and deliberated: AI-Algorithm-Big Data and predictive policing; automated criminal justice system and hyper crime control; surveillance capitalism after singularity and prospects of information civilization[1].

II. Predictive/Automated Criminal Justice and Crime Control

1. Future Crime Control: 21st Century Crime Prediction

There are widespread concerns that predictive policing tools could unintentionally exacerbate over-policing of marginal areas and undermine

TAKEMURA Noriyoshi: Professor, Faculty of Law, Toin University of Yokohama. 1614 Kurogane-cho, Aoba-ku, Yokohama 225–8503, Japan

privacy. Aguirre and others mention that it is widely known that algorithms can reproduce existing patterns of discrimination, reinforcing previous errors and biases of programmers and embedded in databases. There are very real ethical questions about the extent to which such tools can influence police to disproportionately surveil marginalized neighborhoods and communities. There are fears that such tools may augment race and age profiling and undermine privacy rights and civil liberties (Aguirre *et al.*: 8).

There are likewise worries about the ways predictive tools can unfairly target crime offenders and crime victims. For example, they continue, the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) framework which is used by U.S. courts to determine the likelihood that convicted criminals will commit future crime was found to be biased against minorities. Likewise, the Chicago Police Department was subject to intense scrutiny in 2016 when a study conducted by the Rand Corporation found that individuals estimated to be at highest risk of gun violence were neither "more or less likely to become a victim of a homicide or shooting" (Aguirre *et al.*: 9).

In a country with 172 million state-controlled surveillance cameras, they mention, the nation-wide expansion of the initiative can further damage the already battered civil liberties of the Chinese people. The system is said to be imperfect, yielding a large number of false positives when the facial recognition algorithm wrongly identifies a suspect. Experts in law and technology question whether there are due process systems in place to protect citizens from false accusations, and if the false positives are disproportionately skewed toward political dissidents or minority groups (Aguirre *et al.*: 9).

The accelerated pace and spread of crime and violence prediction tools means that these concerns will only grow in the coming years. Indeed, they explain, new platforms are already being tested that aim to automatically classify gang-related crime, combine social media with criminal history to predict crime, and use artificial intelligence to identify individuals with higher risk profiles of committing terrorist acts. The rapid roll-out of these tools invariably raise complex ethical questions in relation to police action and civil rights (Aguirre *et al.*: 9).

Where possible, predictive tools should allow citizens to understand what is inside the 'black box'. While private vendors understandably seek to protect their source code, coupled with their underlying mathematical complexity, this lack of transparency makes it difficult for law enforcement agencies and civil society to understand how the predictions are generated. This can undermine confidence in the tool (Aguirre *et al.*: 10; O'Neil; Ferguson; McCarthy; Van der Sloot *et al.*; Simmons; Selbst).

2. Automated Justice: Algorithm, Big Data, and Criminal Justice Systems

From predictive policing to probation risk scores, the potential uses of big data in criminal justice systems pose serious legal and ethical challenges relating to due process, discrimination, and the presumption of innocence (Collegium Helveticum).

Criminal justice systems are using technological solutions, according to Collegium Helveticum, for instance, to predict future crimes of those applying for bail or those to be sent on a parole. The idea of such 'automated justice' is to vaporize biases, heuristics and to confine fundamentally value-based decisions to 'clean and pure' mathematical reason. There are clear benefits deriving from calculating the risks of misconduct and risk assessments have become relatively standard practice in the criminal systems, e.g. for correctional placement and in the sentencing phase. Such assessment in the sentencing procedure was

utilized long before the development of ICT, but algorithms and big data tools for determining prison sentences or for deciding on a parole are relatively newer practices (Collegium Helveticum).

Researchers have shown how relying too heavily on automated calculations of risk. Such 'automated governance' can lead to 'social sorting on steroids', and can encroach on fundamental liberties, such as privacy and presumption of innocence and even, ultimately, shake the democratic division of power (Collegium Helveticum; Tréguer).

(1) The age of the algorithmic self: the estimological evolution and revolution of the effectiveness movement and automated justice

Risk assessments are increasingly carried out through algorithm-based big-data analysis. It is argued that this method introduces a new frontier of accuracy, to the extent that it may even eliminate all forms of bias. This development represents a significant step forward in the epistemological transition that started with the effectiveness movement in crime control and administrative criminology. Algorithm-based big-data analysis completes this epistemological evolution or, arguably, revolution. If individual-based theories of crime assumed a pathological self, and neoclassical theories assumed a rational self, big-data analysis brings about an 'algorithmic self'. Algorithm-based big-data analysis bypasses consciousness and reason, and offers solutions without concerning itself with the 'path' leading to them ('black box' solutions). In this sense, algorithmic knowledge is a radical break from the types of epistemology that once dominated the modern world, and the knowledge of the world and of the self they produced (Collegium Helveticum).

(2) Automated justice: from the rule of law to the 'rule of algorithm'?

In big data and 'algorithmic' analytics in criminal justice settings, the new language of mathematics is used for blurring contemporary regulatory boundaries, undercutting the safeguards built into regulatory regimes, and abolishing subjectivity and case-specific narratives (O'Neil). The origins of big data in industry and the underlying assumptions, such as "doing more with less," "the numbers speak for themselves" etc., are being transferred to criminal justice system domain where these assumptions have negative consequences for fundamental liberties, such as presumption of innocence and due process of law. With predictive analytics in criminal justice settings, 'big data and algorithms' have changed criminal justice from narrative to database and furthermore towards 'automated decision-making' (Collegium Helveticum).

3. 'Singularity', Crime/Social Control, and its Discontents

The language of big data helps to tear down the walls of criminal procedure rules. Završnik explains that this move towards a system of 'automatic justice' minimizes human agency and undercuts the due process of safeguards built into the traditional criminal justice model. The most far-fetched views contend that big data analytics enables an entirely new epistemological approach to making sense of the world. Such views camouflage big data as an 'objective' and 'pure' knowledge, and neglects the fact that statistics have always been political and served specific political ends. The army of digital workers open to exploitation is used as the means to very specific political ends. There is no 'end of politics' at work here, as the 'reserve army of digital labor' serves the pecuniary interests of the digital industry, which carters to the affluent elite of surveillance society. Digital workers are actually the product being sold on the data market place (Završnik: 4–5).

While being seemingly more objective,

knowledge and neutral language, big data, and algorithms carry several caveats, he analyzes. The mathematical predictions and reasoning used in an increasing number of social domains make the study of big data and algorithms inspiring and frightening at the same time. It is not only the idea of the exponentially increasing computer capabilities heading towards the point of 'technological singularity': the hypothesis that the invention of artificial superintelligence will abruptly trigger runaway technological growth (Kurzweil; Ganascia; Bostrom). There are socially destructive consequences of big data and automated decision-making systems already at work and unfolding in surveillance-based capitalist societies in the form of discrimination against the less affluent and less powerful parts of the population (Završnik: 9, 17–18; Harari).

Big data has been granted too much agency and too much power too quickly, he insists. Big data is shifting power relations in several domains, including control and security. Its predictive potentials have become an attractive method of predicting human behavior in too many contexts, including the improvement of fighting against crime. It has been vested with a great deal of power, while at the same time presents as an objective, value-free scientific tool that requires no transparency or auditing and no further explanation. It has become a projection screen for our desire to predict and colonize the future --- to eliminate all the risks to our well-being, but only for those who can afford a data scientist. Big data may be bringing about a revolution that will transform how we live, work and think, but this revolution will not occur because of big data itself, but because of the specific social, cultural, political and economic imperatives in our society that allow such technology to flourish to detriment of other types of knowledge and social practices (Završnik: 18; The Law Society Commission on the Use of Algorithm in the Justice System and The law Society of England and Wales; Bostrom; Clavel; Mainzer; Kurzweil; Hawking; Harari; Tegmark).

In short, AI that is deployed by and for humans can improve the experience of both people consuming information and those producing it. Without people in the loop, we risk losing the web's fundamental humanity. We must keep people at the center of every policy decision and platform design. We must defend a web that is free and unfettered, and improve connections that allow creativity and collaboration. We should leave the artificial to the machines and restore humanity to the users.

III. 'Surveillance Capitalism' after 'Singularity' and Prospects of Information Civilization

1. Surveillance and Big Data

Big Data intensifies certain surveillance trends associated with information technology and networks, and is thus implicated in fresh but fluid configurations. According to Lyon, this is considered in three main ways: First, the capacities of Big Data (including metadata) intensify surveillance by expanding interconnected datasets and analytical tools. Second, while Big Data appears to be about size, qualitative change in surveillance practices is also perceptible, accenting consequences. Third, the ethical turn becomes more urgent as a mode of critique (Lyon 2014: 1).

Big Data practices echo several key surveillance trends but in several respects they point to realities that have perhaps been underestimated, he analyzes. One is that, within surveillance studies there has been a general tendency to analyze multiple forms of surveillance that are not directly linked with state-based, top-down surveillance of the kind epitomized in George Orwell's *Nineteen-Eighty-Four*. If this was understood by some to mean that more generalized – or, following

Gilles Deleuze, ‘‘rhizomic’’ – surveillance spells less state surveillance activity (Lyon 2014: 10-11; Clavel; Deleuse *et al*.).

In a sense, he insists, this means that Orwell’s bleak vision of what tendencies in post-war liberal democratic polities could lead to authoritarian surveillance regimes were not mistaken so much as standing in need of complementary analyses, such as that of his contemporary, Aldous Huxley, in Brave New World, Big Data practices in consumer surveillance are co-travelers with those of state surveillance and together produce the kinds of outcomes around which ethical debates should now revolve. Indeed, not only are they ‘co-travelers,’ they also cooperate extensively, the one taking methods from the other, with, as discussed above, potentially pernicious results as the ‘successful’ methods in one area are applied in ways deleterious of human rights in another (Lyon 2014: 11).

It is these matters in particular that attract critique, he insists, especially in relation to anticipatory and preemptive approaches common to Big Data mindsets and activities and amplifying what is a long-term surveillance trend. These fit neatly with currently intensifying political styles of neo-liberalism that, with regard to ‘national security,’ are seen in a list towards actuarialism and a consequentialist concern with managing disorder and crime rather than seeking its causes and attempting to eradicate them (Lyon 2014: 11; Lyon 2018; Big Brother Watch; Cheney-Lippold).

2. Surveillance, Facial Recognition, and Right to Obscurity

We have a right to maintain our anonymity such that our mundane activities, behaviors, and associations are not recorded and linked to our identity by means of facial recognition surveillance. Kaplan explains that the mere collection of this non-anonymous data makes us vulnerable to significant harms in the forms of psychological manipulation and opportunity loss. In addition, this right to obscurity is not outweighed by social interests in preventing crime and violence or locating missing persons. These social interests could be equally served while still preserving individuals’ anonymity by dissociating location data from personal identities and by only analyzing behavioral patterns from anonymous data. Since the risks of psychological manipulation and opportunity loss could be greatly reduced by maintaining these protections to public anonymity, implementing facial recognition surveillance without protecting people’s anonymity as obscurity in public would impose an unnecessary and, thus, unjust risk of harm (Kaplan: 18-19).

The right to anonymity as obscurity is here grounded in the broader societal interest within liberal democracies that individuals can effectively exercise their rights and liberties, he continues. The implicit intimidation of using facial recognition surveillance to catalog political and religious participants fails to communicate to individuals that they are not vulnerable to state’s power to impose negative repercussions for their activities and convictions. Given the asymmetry of power between those under surveillance and the institutions carrying out the surveillance, the state has a special obligation to reassure individuals that they will not be subject to negative repercussions when they exercise their rights to free speech, assembly, and worship. Reassurance here can only take the form of banning the use of real-time facial recognition surveillance to catalog participants in political and religious activities. This second right to obscurity while in public is also not overridden by competing social interests. The only justifying purpose for such cataloging is for the sake of a criminal or legal investigation and, for such instances, the real-time use of facial recognition is not required. A warrant can be required to apply this technology post factum to whatever video recordings we have of a crime scene or the like

(Kaplan: 19; Gates; Pellegrini *et al*.).

3. 'Surveillance Capitalism' and Prospects of Information Civilization

Zuboff describes an emergent logic of accumulation in the networked sphere, 'surveillance capitalism', and considers its implications for 'information civilization.' She sheds light on the implicit logic of surveillance capitalism and the global architecture of computer mediation upon which it depends. This architecture produces a distributed and largely uncontested new expression of power: 'Big Other.' It is constituted by unexpected and often illegible mechanisms of extraction, commodification, and control that effectively exile persons from their own behavior while producing new markets of behavioral prediction and modification (Zuboff 2015: 75).

Individuals quickly came to depend upon the new information and communication tools as necessary resources in the increasingly stressful, competitive, and stratified struggle for effective life, she continues. The new tools, networks, apps, platforms, and media thus became requirements for social participation. Finally, the rapid buildup of institutionalized facts – data brokerage, data analytics, data mining, professional specializations, unimaginable cash flows, powerful network effects, state collaboration, hyperscale material assets, and unprecedented concentrations of information power – produced an overwhelming sense of inevitability. These developments became the basis for a fully institutionalized new logic of accumulation that is called surveillance capitalism. In this new regime, a global architecture of computer mediation turns the electronic text of the bounded organization into an intelligent world-spanning organism: Big Other. New possibilities of subjugation are produced as this innovative institutional logic thrives on unexpected and illegible mechanisms of extraction and control that exile persons from their own behavior. Surveillance capitalism offers a new regime of comprehensive facts and compliance with facts. It is a coup from above – the installation of a new kind of sovereign power (Zuboff 2015: 85–86).

The automated ubiquitous architecture of Big Other, she insists, its derivation in surveillance assets, and its function as pervasive surveillance, highlights other surprising new features of this logic of accumulation. It undermines the historical relationship between markets and democracies, as it structures the firm as formally indifferent to and radically distant from its populations. Surveillance capitalism is immune to the traditional reciprocities in which populations and capitalists needed one another for employment and consumption. In this new model, populations are targets of data extraction. This radical disembedding from the social is another aspect of surveillance capitalism's antidemocratic character. Under surveillance capitalism, democracy no longer functions as a means to prosperity but threatens surveillance revenues (Zuboff 2015: 86).

Will surveillance capitalism be the hegemonic logic of accumulation in our time, or will it be an evolutionary deadend that cedes to other emerging information-based market forms? What alternative trajectories to the future might be associated with these competing forms? She concludes that the prospects of information civilization rest on the answers to these questions (Zuboff 2015: 86; 2019a; 2019b; 2021).

In short, the surveillance capitalism threatens to metastasize into a scary new form of power 'instrumentarianism'. The inexorable extension of surveillance technologies, which are so widely used to counter terrorism and serious crime, will overwhelm any hopes we may have of remaining anonymous. In May 2019, San Francisco became the first city in the US to ban the official use of facial recognition technology. We should all be concerned about how such technology is used to police society and we still have the power to shape

the legal framework in which it operates.

IV. Conclusion

Democratic principles should be built into our technologies. This include human rights and human dignity, freedom and self-determination, pluralism and protection of minorities, the division of power, checks and balances, participatory opportunities, transparency, fairness, justice, legitimacy, anonymous and equal votes, as well as privacy in the sense of protection from misuse and exposure, and a right to be let alone. In the future, the principle to be legally and technologically established would be that we decide who is allowed to use what data for what purpose, period of time and price. Uses of personal data, also statistics created for science and for politics, would have to be transparently reported to individuals. We would have to upgrade our system toward a 'multidimensional real-time feedback system'. Such a multidimensional incentive and coordination system is needed manage complex systems more successfully and also to enable 'self-organizing, self-regulating systems'.

[Notes]

1) This article is a part of research results of "Research on North-South Integrated Global Green Criminology and the Foundation of International Environmental Court 2019–2023". This work is supported by JSPS KAKENHI Grant Numbers JP19K01353.

[References]

Aguirre, K., Badran, E., and Muggah, R. (2019). *Future Crime: Assessing twenty first century crime prediction*. Rio de Janeiro: Igarape Institute.

Big Brother Watch (2018). *The State of Surveillance in 2018*.

Bostrom, N. (2014). *Superintelligence: Paths, Dangers, Strategies*. Oxford: Oxford University Press.

Cheney-Lippold, J. (2017). *"We Are Data: Algorithms and the Making of Our Digital Selves"*. New York: New York University Press.

Clavel, G. (-). *La Gouvernance de l'Insécurité : La pénaisation du social dans une societé sécuritaire*. Paris : L'Harmattan.

Collegium Helveticum (2018). *Automated Justice: Algorithm, Big Data and Criminal Justice Systems*. EURIAS-Conference. Zürich: Universität Zürich.

Deleuse, G., et Guattari, F. (1980). *Mille Plateaux: Capitalisme et schizopherénie*. Paris: Les Editions de Minuit.

Ferguson, A. G. (2017). *The Rise of Big Data Policing: Surveillance, Race and the Future of Law Enforcement*. New York: New York University Press.gularite

Ganascia, J.-G. (2017). *Le Mythe de la singularité: faut-il craindre i'intelligence artificiell?* Paris : Éditions de Seuil.

Gates, K. A. (2011). *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York and London: New York University Press.

Harari, Y. N. (2017). *Homo Deus: A Brief History of Tomorrow*. London: Vintage.

Hawking, S. (2018). *Brief Answers to the Big Questions*. London: John Murray.

INTERPOL and UNICRI (2018). *Artificial Intelligence and Robotics for Law Enforcement*.

Kaplan, S. (2018). *To Be a Face in the Crowd: Surveillance, facial Recognition, and a Right to Obscurity*. ECPR Conference 2018.

Kurzweil, R. (2005). *The Singularity Is Near: When Humans Transcend Biology*. London: Duckworth.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data and Society*: 1–13.

Lyon, D. (2018). *The Culture of Surveillance*. Cambridge: Polity.

Mainzer, K. (2016). *Künstliche Inteligenz – Wann übernehmen die Maschine?* Berlin: Springer.

McCarthy, O. J. (2019). *AI and Global Governance: Turning the Tide on Crime with Predictive Policing*.

O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data increases Inequality and Threatens Democracy*. Penguin Books.

Pellegrini, F., et Vitalis, A. (2018). L'ére du fichage généralisé. *Le Monde diplomatique*, avril 2018: 3.

Selbst, A. D. (2017). Disparate Impact in Big Data Policing. *Georgia Law Review* 52: 109–195.

Simmons, R. (2016). Qualifying Criminal Procedure: How to Unlock the Potential of Big Data in our Criminal Justice System. *Michigan State Law Review* 2016: 947–1017.

Tegmark, M. (2017). *Life 3.0: Being Human in the Age of Artificial Intelligence*. Penguin Books.

The Law Society Commission on the Use of Algorithms in the Justice System and The Law Society of England and Wales (2019). *Algorithms in the Criminal Justice System*.

Tréguer, F. (2019). La《ville sure》ou la gouvernance par les algorithmes. *Le Monde diplomatique*, juin 2019: 22–23.

Van der Sloot, B., Broeders, D., and Schrijvers, E. (eds.) (2016) *Exploring the Boundaries of Big Data*. The Hague/Amsterdam: Amsterdam University Press.

Završnik, A. (2018). Big data: What is it and why does it matter for crime and social control? In: Završnik, A. (ed.) *Big Data, Crime and Social Control*. London and New York: Routledge. 3–28.

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology* 30: 75–89.

Zuboff, S. (2019a). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.

Zuboff, S. (2019b). Un capitalisme de surveillance. *Le Monde diplomatique*, Janvier 2019 : 1, 10–11.

Zuboff, S. (2021). The coup we are not talking about. *The New York Times International* February 3: 12, 14.