KULTURA I EDUKACJA

Kultura i Edukacja 2018
No. 4 (122), pp. 94–109
DOI: 10.15804/kie.2018.04.05
www.kultura-i-edukacja.pl

Maciej Gurtowski[1]
Jan Waszewski[2]

Prejudices behind Algorithms: Automated Surveillance Systems as Tools of Segregation and Discrimination[3]

Of course, any time we're judged by algorithms,
there's the potential for false positives
Bruce Schneier (2014)

ABSTRACT
The aim of this paper is to describe the emerging phenomenon of new racism brought by the development of automated surveillance tools. We would like to show that this new system of discrimination is a byproduct of some general transformations in the field of social control. For this purpose, we will refer to invisible hand type of explanation, and the concept of perverse effect in particular. We will also relate widely to some cases and concepts from the "new surveillance" and social control literature and we will try to summarize it.

Keywords:
Big Data, data doubles, dataveillance, invisible hand, new surveillance, perverse effect, racism, surveillant assemblages

The problem of segregation and discrimination is one of the most visible issues present in social sciences. Racism (feeling that someone's race is superior to some-

[1] Institute of Sociology, Nicolaus Copernicus University, Toruń, Poland.
E-MAIL: gurtowski@protonmail.com ORCID: 0000-0002-2990-9088

[2] Center for Security Research, War Studies University, Warsaw, Poland.
E-MAIL: j.waszewski@akademia.mil.pl ORCID: 0000-0002-7370-3714

[3] This paper continues some findings of the research project conducted with NCN financial support that was called: "Correction or deep reconstruction? Human agency from a perspective of neuroscience and foundations of social theory and western culture" (Project signature: DEC-2011/01/B/HS6/01886); see Zybertowicz et al., 2015. The authors would also like to thank Adriana Mica, Hanna Wiśniewska, Stanisław Burdziej, and the two anonymous referees for their insightful comments on an earlier version of this paper.

one else) in sociology is usually understood in relation to prejudices and discrimination. Robert K. Merton (1948/1976, p. 192) created a typology based on those two variables. In his approach, prejudices are attitudes (beliefs) and discrimination is behavior (activity). As a result, four types of people emerge: “unprejudiced non-discriminators”, “unprejudiced discriminators”, “prejudiced non-discriminators”, and “prejudiced discriminators”. It is an important typology, because it highlights that one does not have to be prejudiced to discriminate and that the cause and effect relationship between prejudices and discrimination is not constant.

Thomas C. Schelling, who received the Nobel Memorial Prize in economics in 2005, described “discriminatory behaviour” as “an awareness, conscious or unconscious, of sex or age or religion or colour or whatever the basis of segregation is, an awareness that influences decisions on where to live, whom to sit by” (Schelling, 1971, p. 144). From our perspective the crucial motive of this citation is “conscious or unconscious” basis of people segregation. For instance, programmers do not need to be consciously prejudiced to write a “racist” or discriminatory code. They do not even have to think in racist (discriminating) categories. There are invisible stimuli, unconscious attitudes and institutionalized practices making programmers work (writing codes and algorithms) sensitive towards race (or some other quality). And as Schelling explained in his models, the result of many micromotives, unorganized behaviours of many individuals, is often segregation (i.e., in dwellings; see also O’Neil, 2016).

In short, someone who is not racist, who abhors racism and other forms of discrimination in others, can write algorithms causing discriminatory effects. We call this phenomenon of conscious and unconscious discriminatory behaviours “digital racism” and – we have to emphasize it once more – this phenomenon is not only about race but also about other types of discrimination.

MODERNIZATION AND TRANSFORMATION OF SOCIAL CONTROL

Modern social sciences emerged as an attempt to comprehend the rapid changes occurring in the Western European societies. The role of the newly born discipline was to replace philosophy (and even theology) in their role as a source of interpretations of these changes (Burdziej, 2014). Two centuries ago particular trends were observed – trends that changed the social control in a historically unprecedented way. We can distinguish two trends: the growth of mobility, both vertical and horizontal (Urry, 2007), and the disintegration of traditional communities. Additionally, the increase in urbanization processes has led to a decline of traditional social control based on face-to-face relationships, which was followed by the growing need for depersonalized, professionalized and formally institutionalized social control (Chriss, 2013; Mattelart, 2010). The process of diminishing the role of traditional social control resulted in the emergence of its new forms. Those, in turn, led to the emergence of new techniques of resisting and avoiding social control (Marx, 2009). As a result, a constant and still accelerating arms race continues. The metaphor of an arms race illustrates dynamics in the field of social control. New resistance techniques are followed by better surveillance tools. Among them, automated surveillance systems (Waszewski, 2015) are particularly worth mentioning. Traditional social control is more reactive – people take responsibility for assessing behavior of others (Durkheim, 1893/2014; Foucault, 1977). Modern surveillance systems are more preventive (see: Galetta, 2013), dehumanized, often operating without human input. Modern surveillance systems are a contemporary response to the challenges of a changing world. In this paper we would like to consider some of the consequences of the way they work.

We use sociology of knowledge approach, especially the field of studies called "science, technology, society" (STS). Our aim is not to describe technical aspects of surveillance technologies. They are important for us only as far as they affect the decisions and behavior of actors. For this reason, we propose to treat these specified subsystems of social control, i.e., automated surveillance tools, as a relatively autonomous entity, so-called black boxes (Latour 1987, 1999), internal structure of which is not always clear, but we can still analyse what role they play in broader environment.

NEW SURVEILLANCE

Currently, we are experiencing a tremendous change in the way the social control works. This change is associated with new technologies. The social and technological transformations mentioned above led to the emergence of a phenomenon which was called 'the new surveillance' by social control researchers (Marx, 2002, 2005; Bauman & Lyon, 2013). In traditional social control some cases of violations of important social rules were remembered (sometimes even for centuries) by members of a community. In a new surveillance, however, human memory is supported by archives, files and databases. And human senses are also supported and extended by technical enhancers. Those are not only audio and video recordings, but also tracking and collecting digital traces of our everyday activities.

In opposition to traditional social control, the new surveillance is not based mainly on repression. The aim is rather to prevent and even anticipate violations (preemptive actions). Traditional social control focuses more on individuals who are defined as dangerous. New surveillance, on the other hand, works constantly, collecting data on the whole social contexts. The best example which show how new surveillance works are security systems on airports (Salter, 2008). Finally, a key change in the transformation of social control is its process of automation, in particular, the automation of assessment of people.

In the current surveillance studies, the role of Big Data systems in surveillance (more about this phenomenon in following section) is being analysed to a great extent. The disclosure, whistle-blowing by a former officer of the American NSA Edward Snowden, was a turning point in the assessment of this technology from the point of view of surveillance and society (Bauman et al., 2014). From this moment scholars' attention is more often than not focused on the challenges and risks associated with the emergence of a new type of totalitarianism based on total surveillance (Lyon, 2015). Big Data is perceived as the threat to privacy, civil liberties and civic agency, i.e., results of self-surveillance practices (Klauser & Albrechtslund, 2014; O'Neil, 2016).

DATAVEILLANCE AND BIG DATA

Since the eighties of the last century the role of computer databases in surveillance has been noticed. Some researchers use the concept of 'dataveillance' introduced in 1988 by an Australian scientist Roger Clarke (1988). His concept is related to the belief that social control in modern society is based on information technology, which allows for the collection, storage and processing of data in digital format. Dataveillance is a merger of two concepts – digital data processing technologies and surveillance.

Digital or digitalized data created in present day can be stored in databases and processed according to the needs. This phenomenon is collectively described by the "catchphrase" – the Big Data.

Usually Big Data is being defined by so called „4Vs". Those are Volume, Velocity, Variety, and Veracity (or, in other definitions, Value) (see, i.e., Gandomi & Haider, 2015). In short: (1) databases are enormous and still growing (Volume); (2) they can be fed with new data in real time, accessed in real time and give analytical added value in real time, too (Velocity); (3) new ways of constructing databases allow storage and usage of different kinds of digital data (also unstructured and in diverse formats) (Variety); (4) analysis of such databases provides an organization actionable and useful knowledge (Veracity), that gives them chance to earn more (Value).

Big Data is in fact synonymous with enormous storage of data and, at the same time, with tools (algorithms) analysing those data (Needham, 2013). Big Data, it is said, transforms society (Mayer-Schönberger & Cukier, 2014). Between others, Big Data creates new ways of enforcing social control (as we mentioned in the previous section).

The crucial element of dataveillance phenomenon is identifying people (see: Lyon, 2009). In 1988, when concept of datavaillance was coined, there was a difference between personal (aimed at known individuals) and mass dataveillance (aimed at groups) (Clarke, 1988). In one of the following sections we are going to describe the process of creation of ‘data doubles’. This process is in fact personal dataveillance – collecting all information about individuals and building their digital dossiers. At the same time, Big Data is causing qualitative changes. Nowadays, there is no need to stop collecting data because we are running out of storage space or to choose only some types of data. The promise of Big Data is as follows: you can collect everything, analyse it all and because of analytical algorithms and the scale effect, you will get results (Mayer-Schönberger & Cukier, 2014).

In the cited above classical text about dataveillance there are whole sections about ‘real and potential dangers of dataveillance’ (Clarke, 1988). When we are reading this today, 30 years later, it is like going through the list of issues that present day anti-surveillance watch-dogs are investigating. Blacklisting as a tool of blocking access to some services is a good example of such issues. In an instance of accidently occurring mistake, one can be automatically removed from the list of job applicants. Even in an instance when someone in fact has had a history of misdeeds, they are not able to redeem themselves. Digital data is hard to erase and finding primary sources of that information is even harder. Bad reviews (i.e., from Ebay or hotel visitors) do not disappear and in some cases are ruining reputation of the reviewees even many years later[4]. Clarke’s text from 1988 dissects credit history – this concept has spread to other spheres of our everyday lives (Pasquale, 2015). The communist rulers of China are trying to “rebuild trust in society” by creating automated system of “citizen score” (Meissner, 2017). This system is based on adding and deducting points for behaviours/activities classed as pro- and anti-social. In 2021, every citizen of China should have between 0-

[4] The UE’s law “the right to be forgotten” helps only in some instances.

1000 points. According to Chinese authorities, the citizen score is going to award those who have enough points and punish those who are below some arbitrarily set level.

The companies and government agencies controlling Big Data systems are hungry for data. At the same time, they are not eager to explain, how those systems work and how they are making decisions. Algorithms decide about people's lives, but they are often trade or state secrets. More and more often algorithms make life altering decisions, but we do not know how exactly they do it (Meissner, 2017; O'Neil, 2016). Thus, algorithms have become regulators of many aspects of social life.

SURVEILLANT ASSEMBLAGES

Among the metaphors used by surveillance researchers, the metaphor of surveillant assemblages seems particularly valuable (Haggerty & Ericson, 2000). We shall omit the philosophical sources of this idea, but assemblage is also an archaeological concept. It means that one cannot analyse some objects without their context. The archaeological findings can only be explained after the reconstruction of their environment (surrounding artefacts and their relations to each other).

If we want to understand surveillance systems, we have to treat them as assemblages. They grow in a way that makes it impossible to understand them without recognizing interconnections and relationships of various systems. For example, surveillance systems of government and private companies interact and collaborate in public-private partnerships (Lahav, 2008; Maki, 2011). Human activities are observed and recorded also in situations and by tools that were not meant to support social control. But eventually they have become part of the surveillant assemblage because they were used to influence human behaviour.

Surveillance system has been described by an influential author in field of surveillance studies David Lyon (2003, p. 31) as assemblage:

> “it seems to account for dispersal, decentralization, and globalization of surveillance. The assemblage, in this context, is a set of loosely linked systems […]. It is emergent and unstable. It operates across state institutions and others that have nothing (directly) to do with the state. From the point of view of data-subject, this relates to our daily experiences of surveillance, which occur in mundane moments rather than in special searches”.

With reference to Robert Nozick, we can say that surveillant assemblage “looks to be the product of someone's intentional design, as not being brought about by anyone's intentions" (Nozick, 1974, p. 19). Nozick also (1991, p. 314) distinguishes two mechanisms in which such an unexpected entity can occur from a set of actions and intentions not aiming at it, between others: "equilibrium processes wherein each component part adjusts to local conditions, changing the local environments of others close by, so the sum of the local adjustments realizes a pattern". This is similar to the dynamics of an assemblage.

We have already referred to the case of information disclosed by Snowden in 2013. The US electronic intelligence agency (NSA) and its allies in various programs used the data and metadata created by the users of social media and ICT (Information and Communication Technologies). We could refer to multiple examples, but in fact only one issue seems crucial for us here. To understand how the surveillance works, you have to look at the consequences of technology development. More and more of the everyday devices leave digital traces. Databases are becoming larger and are more effectively used. As a result, dataveillance can be understood from the point of view of surveillance as assemblages.

CREATION OF 'DATA DOUBLES'

We have already mentioned personal dataveillance as an example of the way the Big Data and databases can be used to collect all available digital information (digital dossier) about a particular person. We call this phenomenon the creation of 'digital doubles' (Haggerty & Ericson, 2000).

This is a serious philosophical, ontological matter: who is more real in the modern world – man of flesh and blood, or his digital equivalent? Which one will be evaluated when there is a need to establish someone's reputation?

We should keep in mind that more and more often people are being evaluated by computer systems; they are in fact evaluating their digital doubles. There is a promise: computers are objective, non-prejudiced and they will not discriminate anyone; nevertheless the way the algorithms work is often opaque also for their programmers. Moreover, even if someone can analyse the way they work it usually has a status of a trade secret (Mayer-Schönberger & Cukier, 2014; Pasquale, 2015). Furthermore, Big Data systems are finding out information about people they would prefer to keep hidden (Stephens-Davidowitz, 2017).

The question is: what if the result of algorithm performance is a racist Big Data system (see: Brennan, 2015)? The well known example is bias in online advertisement delivery by Google. Latanya Sweeney from Harvard University found out that names usually belonging to Black people, when they were searched on Google, “generated ads suggestive of an arrest” (2013). “White” first names generated more neutral advertisement.

It does not always have to be the result of programmer’s prejudice. More often now than ten years ago, it is the machine learning that makes the algorithms “learn” biases, because they were present in the data (Hardt, 2014; Angwin et al., 2016). Thus real world prejudices enter the world of “objective” algorithms. As Andrew G. Ferguson (2017) stated in his book “The Rise of Big Data Policing” – criminal data just has a colour.

There is an interesting case of asylum and migration decision-making in Australian border automated control system (Wilson & Weber, 2008; Kenk et al., 2013). Australian authorities have hidden discriminating racial criteria in a complex system of migrants’ assessment. Algorithms of this system were based on: “risk profiling, social sorting and ‘punitive pre-emption’” (Wilson & Weber, 2008, p. 124). How often the decision (“low risk” vs. “high risk”) about people crossing boarders or travelling by air are made by algorithms with built in biases causing segregation and discrimination (in other words: digital racism)? What if Big Data analytics would recognize – without biased programmers intervention – race as an indicator of probable future wrongdoings? What if race is an unavoidably associated variable found out during assessment of migrants? Should we exclude algorithms only because they take race into account?

THE NEW SYSTEM OF DISCRIMINATION WITHOUT SUBJECT

The new system of discrimination is not directly based on discriminatory practices. It is separated from a human subject while it influences human objects. Furthermore, we would like to underline that there is a striking contradiction between common public image of the automated surveillance systems and their performance. Surveillance assamblages are amorphic structures that cannot be fully intentionally managed. Also the “population” of data doubles emerged rather spontaneously through our everyday actions and through digital traces we left. As David J. Gunkel (2014) recently indicated, “terms of service agreements” do not protect privacy – people who are encouraged to sign it by clicking “I agree” do not understand consequences of their consent.

As we mentioned in the introduction, one of the criteria for distinguishing the surveillance of a new type from traditional social control is its preemptive nature, predictive policing for instance (Klauser & Albrechtslund, 2014; Ferguson, 2017), and preventing norms’ violation. The key procedure in this type of action is profiling (van Otterlo, 2014), in other words, comparing particular cases to a certain pattern of activities defined as dangerous for social order. The most important factor is the origin of this pattern. Following procedures of automated comparison-making is presented as an activity that is objective and impartial. On the other hand, however, there are real people "behind the algorithms". Those programmers and controllers of automated surveillance systems are usually under influence of biases and prejudices (Curry, 2003; Searle, 2003; Schneier, 2014). American surveillance researcher Nancy D. Campbell points out that algorithms of surveillance systems are being often written in the way that helps in collecting data that confirms pre-assumptions of the discriminatory nature (Campbell, 2004; see: Guzik, 2009).

Similarly, consequences of the face recognition system used in the CCTV network are being criticized by Lucas D. Introna and David Wood (Introna & Wood, 2004). Also Christel Backman draws attention to the misuse of databases of criminal records by employers in Sweden (Backman, 2012). Generally, the problem is related to the broader phenomenon known as "technologisation of security" (Ceyhan, 2008). Anthony Newkirk writes about the present dangers in the context of analytical data "fusion centers" (where data from many sources is being analysed) working for the justice and law enforcement agencies in the US: "While the official purpose is to protect public safety, the practice of 'data-mining' and unclear lines of authority lead to fusion centers being unaccountable to the public and, hence, a threat to the democratic process" (Newkirk, 2010, p. 43).

This new automated system of people assessment, social sorting, segregation and discrimination has the following features:

- The criterion of discrimination is not an attribute of a physical person but of his 'data double'.
- The effect of this discrimination means exclusion from some social contexts.
- The subject of discrimination is not a person or a group, it is depersonalized system or procedure.
- By the same time, this system is presented as objective and impartial.
- The racist social practice occurs but without racists involved.
- Discriminating system is opaque. It operates as a black box. Its internal mechanisms of classification are unclear.
- Automated surveillance systems are not given or do not appear *ex nihilo*. They are made by humans. Racial and other prejudice could be implemented initially by algorithms creators ("prejudiced discriminators" or "unprejudiced discriminators"), who did that consciously or unconsciously; and in more complex algorithms, prejudices could be added or developed in the process of machine learning.

The symbol and personification of the judicial system is like blind Themis, who assesses people and their deeds. Meanwhile, the problem observed in the literature indicates a specific trend, which seems to arise from a question, whether the scales of Themis (human judicial decision making) should be replaced with a computer, as it might be able to generate fairer judgments or help in making them.

From the general point of view, the key precondition to the effectiveness of control systems lays in the acceptance of strong legitimizing assumption. The first one presumes that automated surveillance algorithms are objective and impartial.

The crucial problems are the algorithms' creators biases (Kang et al., 2012) against certain groups, types of people and minorities (Tetlock & Mitchell, 2006). It is pointed out that prejudice of this kind should not affect their work, but biases are common and they cannot be eliminated, because they are often examples of automaticity in social cognitive processes, as well as habits (Kolańczyk, 2009; see: Duhigg, 2013).

Let's look at the discrimination as a social institution. Traditional forms of discrimination were based on some recurrent pattern of behaviour (aimed at maintaining social inequalities). The emerging forms of digital racism are also indirectly supported by our everyday online activity. We assume that this new system of discrimination emerged spontaneously at the beginning, but there is evidence that it is now supported by some influential actors.

Just consider the following case – independent Internet newsroom "ProPublica" (based in New York) published in October 2016 investigative article about exclusion of minorities from looking at Facebook advertisements (Angwin & Parris, 2016). While ordering the advert, advertisers could decide that they did not want to show their offer to members of some ethnic groups. Facebook of course knows well what its users races are – even if they do not share this information, they will leave enough traces to infer colour of their skin and ethnicity. Facebook asked simple and usually standard question: whom would you like not to show your ad to? The consequence was serious. Facebook has been helping in creating segregated neighbourhoods or – at least – company made such process easier. Moreover other advert platforms, i.e., the "The New York Times", use special automated filters to stop "whites only" or "no kids" and even "no churches" announcements. At the same time Facebook has been found out as involuntarily racist organization. The way to solve this problem was Facebook's "privacy and public policy manager" declaration about building automated system searching for illegal adverts (Angwin, 2016).

Practice that is believed to be impartial, in fact is even more discriminatory. That is why we would like to call this process a perverse effect – in a meaning that is close to Raymond Boudon. He wrote: "The perverse mechanisms that are most significant socially are those that end up producing *undesirable* effects, those that are in every parlance called perverse. By creating unwanted and often unexpected social imbalances, they play a vital role in social change. […] They [individuals] may attain their individual objectives but produce collective ills as well" (Boudon, 1982, pp. 5–6). Boudon also stated, which is especially relevant in our case, that "Technical progress, which is an indisputable feature of industrial societies, provides the occasion for new forms of perverse effect to develop" (Boudon, 1982, p. 8).

We aim to demystify the illusion of objectivity and impartiality of automated surveillance systems. People are not always rational and usually are not independent from external influences. The creators of algorithms steering automated surveillance systems should focus on their own pre-assumptions in their attitudes toward new technologies. Only understanding of how those pre-assumptions influence them could possibly induce algorithms' creators to be a bit more objective. This understanding might encourage them to make more informed decisions regarding the development and usage of tools that, as an end result, are going to affect both, the people and data, equally.

It appears to be a wider area for exploration, for example, who the algorithm creators are? Are they mostly members of so called 'digital upper class' or more like 'digital proletariat'? Particular attention should be given to the process of emergence and the reproduction of a common social ontology present in their professional subculture. Moreover, the general public do not know who is defining the rules of segregation. Who is giving orders to algorithms' creators? Who decided that after the 9/11 people of Arabic phenotype are more risky than others (see: Guzik, 2009)? Is this really only the case of spontaneous emergence of surveillant assemblage?

We want to create a "warning forecast", which indicates that we need to watch the upcoming changes in the area of social control. We do not want to be surprised by them and fall into the trap of judging people on the unjust basis, based on unclear rules. That could easily lead to some form of "new totalitarianism". The narrative implying objectivity of automated technologies should not be taken for granted without deeper understanding. It seems crucial to find out who the creators and purchasers of surveillance systems are, and what their agenda is. Perhaps if surveillance algorithm creators were more conscious of the multidimensional nature of their work, there would be more whistle blowers following steps of Edward Snowden.

WHY NEW SURVEILLANCE CAUSES DISCRIMINATION?

Among important features of new surveillance, beside its apparent impartiality and independence, there is opaqueness. New surveillance systems become black boxes – term used by Bruno Latour to describe relatively isolated entities that are important parts of social practices. But at the same time, people are not conscious of what actually occurs inside the black box. We know input, and output of the black box, but we do not know what the mechanisms inside it are. In our opinion, the main thing is that we do not need to know everything to use the black box "properly". And, to be honest – this knowledge could destroy the effectiveness, the utility of the black box, by revealing, for example, its brutality, or its bad influence on the environment. It is very hard to force people to get rid of the black box once it is engaged in supporting someone's interests.

Therefore, we propose to consider two hypothetical explanations which could clarify why new surveillance brings new forms of social segregation and discrimination. We are of the opinion that the effectiveness of the new surveillance systems is not strictly dependent on the use of advanced technologies. We also admit that the practical effectiveness of the new surveillance lays in fact that it enables the restitution of some discriminating practices, whilst being invulnerable to accusations of being unfair. From the social control point of view, prejudices are just functional.

Explanation no 1 (weak approach): There is hidden potential for discrimination in modern western societies that is unleashed by automatic surveillance systems. At a level of collective unconsciousness, repressed attitudes toward strangers are easy to restitute. It is so because discrimination petrifies social hierarchy. Therefore, automatic surveillance systems support the interests of the elites, most influential actors and interest groups.

Explanation no 2 (strong approach): Discrimination is an element of social control system of the modern society. In the past, when traditional social control dominated, it was easier to recognize strangers and to separate them from "ours". Now, when segregation and discrimination has been stigmatized, such recognition and isolation has to be done by other means. Stigmatization of prejudices does not eliminate them. Without a risk assessment, based on assessment of people, without dividing people into categories, social control cannot fulfill its function.

Prejudices are not eliminated from social control mechanisms. Instead people labeled as prejudiced are now to some extent eliminated from public attention. But prejudices still persist hidden behind algorithms. At the end, we could conclude with a following metaphor: curbing discrimination is futile to some extent, so if you throw out discrimination through the door it will come back through the window. It will just be redressed in the new garments. Thus it might be even stronger and less vulnerable to be thrown out again.

References

Angwin, J. (2016). Facebook Says It Will Stop Allowing Some Advertisers to Exclude Users by Race. *ProPublica*, November 11. Retrieved from: https://www.propublica.org/article/facebook-to-stop-allowing-some-advertisers-to-exclude-users-by-race.

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine Bias. *ProPublica*, May 23. Retrieved from: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

Angwin, J., & Parris Jr., T. (2016). Facebook Lets Advertisers Exclude Users by Race. *ProPublica*, October 28. Retrieved from: www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race.

Backman, C. (2012). Mandatory Criminal Records Checks in Sweden: Scandals and Function Creep. *Surveillance & Society*, 10(3/4), pp. 276–291. DOI: 10.24908/ss.v10i3/4.4206.

Bauman, Z., & Lyon, D. (2013). *Płynna inwigilacja. Rozmowy*. Kraków: Wydawnictwo Literackie.

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R.B.J. (2014). After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology*, 8(2), pp. 121–144. DOI: 10.1111/ips.12048.

Boudon, R. (1982). *The Unintended Consequences of Social Action*. Berlin, New York: Springer.

Brennan, M. (2015). Can Computers Be Racist? Big Data, Inequality, and Discrimination. *Equals Change Blog*, November 18. Retrieved from: http://www.fordfoundation.org/ideas/equals-change-blog/posts/can-computers-be-racist-big-data-inequality-and-discrimination/.

Burdziej, S. (2014). Sociological and Theological Imagination in a Post-secular Society. *Polish Sociological Review*, 2(186), pp. 179–193.

Campbell, N.D. (2004). Technologies of Suspicion: Coercion and Compassion in Post-disciplinary Surveillance Regimes. *Surveillance & Society*, 2(1), pp. 78–92.

Ceyhan, A. (2008). Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics. *Surveillance & Society*, 5(2), pp. 102–123.

Chriss, J.J. (2013). *Social Control: An Introduction*. 2nd Ed. Cambridge: Polity Press.

Clarke, R. (1988). Information Technology and Dataveillance. *Communications of the ACM*, 31(5), pp. 498–512. DOI: 10.1145/42411.42413.

Curry, M.R. (2003). The Profiler's Question and the Treacherous Traveler: Narratives of Belonging in Commercial Aviation. *Surveillance & Society*, 1(4), pp. 475–499. DOI: 10.24908/ss.v1i4.3332.

Duhigg, C. (2013). *The Power of Habit: Why We Do What We Do, and How to Change*. London: Random House.

Durkheim, É. (1893/2014). *The Division of Labor in Society*. New York: Simon and Schuster.

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

Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison.* New York: Vintage Books.

Galetta, A. (2013). The Changing Nature of the Presumption of Innocence in Today's Surveillance Societies: Rewrite Human Rights or Regulate the Use of Surveillance Technologies? *European Journal of Law and Technology*, 4(2).

Gandomi, A., & Haider, M. (2015). Beyond the Hype: Big Data Concepts, Methods, and Analytics. *International Journal of Information Management*, 35(2), pp. 137–144. DOI: 10.1016/j.ijinfomgt.2014.10.007.

Gunkel, D.J. (2014). Social Contract 2.0: Terms of Service Agreements and Political Theory. *Journal of Media Critiques*, 2, pp. 145–167. DOI: 10.17349/jmc114208.

Guzik, K. (2009). Discrimination by Design: Data Mining in the United States' 'War on Terrorism'. *Surveillance & Society*, 7(1), pp. 1–17.

Haggerty, K.D., & Ericson, R.V. (2000). The Surveillant Assemblage. *The British Journal of Sociology*, 51(4), pp. 605–622. DOI: 10.1080/00071310020015280.

Hardt, M. (2014). How Big Data Is Unfair. *Medium*, September 26. Retrieved from: https://medium.com/@mrtz/how-big-data-is-unfair-9aa544d739de.

Introna, L.D., & Wood, D. (2004). Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems. *Surveillance & Society*, 2(2/3), pp. 177–198.

Kang, J., Bennett, M., Carbado, D., Casey, P., Dasgupta, N., Faigman, D., Godsil, R., Greenwald, A.G., Levinson, J., & Mnookin, J. (2012). Implicit Bias in the Courtroom. *UCLA Law Review*, 59, pp. 1124–1186.

Kenk, V.S., Križaj, J., Štruc, V., & Dobrišek, S. (2013). Smart Surveillance Technologies in Border Control. *European Journal of Law and Technology*, 4(2).

Klauser, F.R., & Albrechtslund, A. (2014). From Self-tracking to Smart Urban Infrastructures: Towards an Interdisciplinary Research Agenda on Big Data. *Surveillance & Society*, 12(2), pp. 273–286. DOI: 10.24908/ss.v12i2.4605.

Kolańczyk, A. (2009). Procesy świadome a automatyzmy w poznaniu społecznym. In: M. Kofta, & M. Kossowska (Eds.), *Psychologia poznania społecznego. Nowe idee* (pp. 31–57). Warszawa: Wydawnictwo Naukowe PWN.

Lahav, G. (2008). Mobility and Border Security: The US Aviation System, the State, and the Rise of Public-Private Partnerships. In: M.B. Salter (Ed.), *Politics at the Airport* (pp. 77–103). Minneapolis: University of Minnesota Press.

Latour, B. (1987). *Science in Action: How to Follow Scientists and Engineers through Society.* Cambridge, Mass: Harvard University Press.

Latour, B. (1999). *Pandora's Hope: Essays on the Reality of Science Studies*. Cambridge, Mass: Harvard University Press.

Lyon, D. (2003). *Surveillance After September 11.* Cambridge: Polity.

Lyon, D. (2009). *Identifying Citizens: ID Cards as Surveillance*. Cambridge: Polity Press.

Lyon, D. (Ed.). (2011). *Theorizing Surveillance: The Panopticon and Beyond.* London and New York: Routledge Taylor and Francis Group.

Lyon, D. (2015). The Snowden Stakes: Challenges for Understanding Surveillance Today. *Surveillance & Society*, 13(2), pp. 139–152.

Maki, K. (2011). Neoliberal Deviants and Surveillance: Welfare Recipients under the Watchful Eye of Ontario Works. *Surveillance & Society*, 9(1/2), pp. 47–63.

Marx, G.T. (2002). What's New About the 'New Surveillance'? Classifying for Change and Continuity. *Surveillance & Society*, 1(1), pp. 9–29. DOI: 10.24908/ss.v1i1.3391.

Marx, G.T. (2005). Surveillance and Society. In: G. Ritzer (Ed.), *Encyclopedia of Social Theory*, Vol. 2 (pp. 816–821). Thousand Oakes, London, New Delhi: Sage Publications.

Marx, G.T. (2009). A Tack in the Shoe and Taking Off the Shoe: Neutralization and Counter-neutralization Dynamics. *Surveillance & Society*, 6(3), pp. 294–306. DOI: 10.24908/ss.v6i3.3286.

Mattelart, A. (2010). *The Globalization of Surveillance: The Origin of the Securitarian Order*. Cambridge: Polity.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: a Revolution That Will Transform How We Live, Work, and Think*. Eamon Dolan/Mariner Books.

Meissner, M. (2017). *China's Social Credit System: a Big-Data Enabled Approach to Market Regulation with Broad Implications for Doing Business in China*. May 24. Retrieved from: https://www.merics.org/sites/default/files/2017-09/China%20Monitor_39_SOCS_EN.pdf.

Merton, R.K. (1948 /1976). Discrimination and the American Creed. In: R.K. Merton, *Sociological Ambivalence and Other Essays* (pp. 189–216), New York: The Free Press.

Needham, J. (2013). *Disruptive Possibilities: How Big Data Changes Everything*. Bejing, Cambridge, Farnham, Koln, Semastopol, Tokyo: O'Reilly Media.

Newkirk, A.B. (2010). The Rise of the Fusion-Intelligence Complex: a Critique of Political Surveillance after 9/11. *Surveillance & Society*, 8(1), pp. 43–60. DOI: 10.24908/ss.v8i1.3473.

Nozick, R. (1974). *Anarchy, State, and Utopia*. Malden, Mass: Basic Book.

Nozick, R. (1991). Invisible-Hand Explanations. *The American Economic Review*, 84(2), pp. 314–318.

O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown Publishers.

Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge: Harvard University Press.

Salter, M.B. (Ed.). (2008). *Politics at the Airport*. Minneapolis: University of Minnesota Press.

Schelling, T.C. (1971). Dynamic Models of Segregation. *Journal of Mathematical Sociology*, 1, pp. 143–186. DOI: 10.1080/0022250X.1971.9989794.

Schneier, B. (2014). NSA Robots Are 'Collecting' Your Data, Too, and They're Getting Away with It. *The Guardian*, February 27. Retrieved from: https://www.theguardian.com/commentisfree/2014/feb/27/nsa-robots-algorithm-surveillance-bruce-schneier.

Searle, R.H. (2003). Organizational Justice in E-recruiting: Issues and Controversies. *Surveillance & Society*, 1(2), pp. 227–231. DOI: 10.24908/ss.v1i2.3357.

Stephens-Davidowitz, S. (2017). *Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us About Who We Really Are*. New York: Dey Street Books.

Sweeney, L. (2013). Discrimination in Online Ad Delivery. *Communications of the ACM*, 56(5), pp. 44–54.

Tetlock, P.E., & Mitchell, G. (2006). Antidiscrimination Law and the Perils of Mindreading. *Ohio State Law Journal*, 67(5), pp. 1023–1121.

Urry, J. (2007). *Mobilities*. Cambridge, Malden: Polity.

Van Otterlo, M. (2014). Automated Experimentation in Walden 3.0: The Next step in Profiling. *Surveillance & Society*, 12(2), pp. 255–272. DOI: 10.24908/ss.v12i2.4600.

Waszewski, J. (2015). Ewolucja systemów nadzoru. In: A. Zybertowicz, M. Gurtowski, K. Tamborska, M. Trawiński, & J. Waszewski, *Samobójstwo Oświecenia? Jak neuronauka i nowe technologie pustoszą ludzki świat* (pp. 233–284). Kraków: Wydawnictwo Kasper.

Wilson, D., & Weber, L. (2008). Surveillance, Risk and Preemption on the Australian Border. *Surveillance & Society*, 5(2), pp.124–141. DOI: 10.24908/ss.v5i2.3431.

Zybertowicz, A., Gurtowski, M., Tamborska, K., Trawiński, M., & Waszewski, J. (2015). *Samobójstwo Oświecenia? Jak neuronauka i nowe technologie pustoszą ludzki świat*. Kraków: Wydawnictwo Kasper.