Chapter 1

The algorithmic society

An introduction

Rik Peeters and Marc Schuilenburg

How will they shape you?

Algorithms are everywhere, from simply suggesting online search results or friends 'you may know' on social media, to more critical matters like helping doctors determine your cancer risk, to decide whether you can have a mortgage, or to predict crimes such as gang violence and burglary. Because it is so hard to spot, you might not have even noticed how much of our life is influenced by algorithms. The content we consume on Facebook, the music we listen to on Spotify, the movies we watch on Netflix – it relies on predictive modelling by algorithms. With each click, the algorithms learn to personalise their 'feed' and the marketing for our best experience. Although many of these examples are driven by commercial interests, they are also used in the public sector, such as in health care, education, criminal justice and tax administration. Public organisations increasingly use new forms of data analysis in order to improve public services. We find algorithms used by judges to decide whether a criminal defendant is likely to reoffend or not. We see algorithms used by municipalities to identify optimal routes for waste collection. We encounter algorithms used by teachers for assigning students to schools. Algorithms are here to stay and – the story goes – to help us. The idea is that algorithms are a solution to the mayor challenges of our time, such as security, public services, health care, and environmental protection.

We are living in the midst of a significant transformation of our lives, and while it is an incredible time and place to be in, we must be wary of the effects that come along with it. Mind-boggling amounts of data are generated regarding our daily actions with algorithms processing and acting upon these data to make decisions that manage, control, and nudge our behaviour in everyday life. The use of algorithms not only expands the possibilities of current control and surveillance, but also introduces a new paradigm characterised by an increased rationality of governance, a shift in the functioning of power, and closure of decision-making procedures. We can refer to this by using the term 'algorithmic governance' – the replacement of human, legible and accountable judgements with 'black-box' algorithms – or, as sociologist Aneesh Aneesh dubbed it, 'algocracy' (2006, 2009; Engin & Treleaven, 2019). The term 'algorithmic governance' signifies three distinctive, but related elements with a direct bearing on our behaviour. While automation in decision-making is not

particularly new, the impact of algorithms is increasingly becoming *systemic* in terms of (1) automation; (2) architecture; and (3) anticipatory applications.

Full *automation* means that human agency can be almost completely designed out of decision-making processes – even though the extent to which this happens varies in practice. Algorithms collect information (input), process it (throughput), apply it (output) and learn to improve output (feedback) (Zarsky, 2013; Citron & Pasquale, 2014; Danaher et al., 2017). Artificial intelligence, databases, websites, and automated procedures are replacing human agency from actual decision-making (Henman, 2010; Peeters & Widlak, 2018; Van der Voort et al., 2019). Moreover, decision-making becomes a matter of classification rather than judgement of individual cases (Peeters & Schuilenburg, 2018). As a consequence, new actors or experts are now entering the game (usually not trained in social sciences). The discretionary space shifts to the IT professionals that design algorithms, to the data analysts that identify behavioural patterns, and in a certain way also to the algorithms themselves that recognise new patterns and adjust their decision-making procedures accordingly through machine learning (Hannah-Moffat, 2019).

Moreover, algorithms are not merely embedded in existing organisational practices or procedures, but instead form the core of an information *architecture* that determines to a large extent how commercial organisations and public services operate. The widespread use of algorithms fits into a historical development of the digitalisation of organisational operations. In the 1980s, information technology was used primarily to convert organisational documentation into standardised and printable formats. A next step was the digitalisation of files and information into databases, which then could be used to digitalise decision-making procedures and organisational analytics. Pre-filled tax returns are a classic example of this development. Organisational practices changed accordingly. Computer screens replaced paper and system-level information technology replaced individual decision-making based on formal-legal procedures (Bovens & Zouridis, 2002; Landsbergen, 2004). The most recent development is the use of information technology to share data among networks of organisations. Automated decisions by one organisation can now be based on information coming from another organisation, which not only implies the harmonisation of technology (Olson & Subodh, 2010) but can also include the harmonisation of definitions, classifications, and legal frameworks (Widlak & Peeters, 2018). Algorithms – which form the core of digital data sharing and decision-making procedures – should, therefore, be understood as part of a broader information architecture (cf. Yeung, 2011, 2018). Supra-organisational information systems function as an infrastructure that allows for the free flow of information but also guides and constrains its use (Bowker & Star, 2000; Cordella, 2010).

Finally, the application range of algorithm-based organisational practices has expanded considerably in recent years. Most importantly, algorithms are no longer merely used to automate existing internal procedures but, instead, play a key role in new forms of governing society. In the examples given above, algorithms are used to predict, nudge or constrain human behaviour (Danaher et al., 2017). They do so through scores, rankings, profiles and patterns. In 'surveillance capitalism' (Zuboff, 2019), analysis and prediction of client behaviour is a powerful business

model that underpins the digital world and is applied in e-commerce, by credit card companies and by social media platforms such as Facebook and Google (Mayer-Schoenberger & Cukier, 2013). The 'proliferation of scoring and ranking citizens' (Harcourt, 2015: 205) also extends to the public domain, where algorithmic risk assessments are used for making no-fly lists, for probation decisions (Smith, Bennett Moses & Chan, 2017: 260), for determining police surveillance resource allocation (Bennett Moses & Chan, 2018), or for algorithmically producing the 'other' as an anomaly in big data analysis (Aradau & Blanke, 2017). Here, algorithmic *anticipation* highlights behavioural patterns and profiles by reducing humans and their behaviour to a set of variables – such as age, gender, educational level, consumer behaviour, criminal record, and income. Individuals have become 'dividuals' (Deleuze, 1990), persons who are defined by the data sets that profile and predict their conduct. As a consequence, the paradigm of the autonomous and sovereign subject no longer serves as a heuristic point of departure. (In)dividuals are entities with many roles, represented in different data banks (Koopman, 2019).

Understanding algorithms

Algorithmic governance is central to the functioning of public and private organisations. For instance, police forces use them to predict where, when and by whom crimes are more likely to be committed (Perry et al., 2013; Asquer, 2014; Van Brakel, 2016; Smith & O'Malley, 2017; Williams, Burnap & Sloan, 2017; Bennett Moses & Chan, 2018). In criminal justice, algorithms are used to predict future dangerousness of defendants and convicts (Sjöstedt & Grann, 2002; Kleiman, Ostrom & Cheeman, 2007; Berk, 2012; Berk & Bleich, 2013; Hamilton, 2015; Goel, Rao & Shroff, 2016; Douglas et al., 2017). Marketeers use algorithms to analyse consumer audiences from online search queries, credit card purchase data, and behavioural data (Sadin, 2009; Mager, 2012; Reigeluth, 2014; Harcourt, 2015; Zuboff, 2019). Government agencies are turning towards algorithms to, among other things, identify welfare fraud, deliver public services, allocate regulatory oversight resources, and assess risks in child protection (Coglianese & Lehr, 2017; Van Eck, 2018; Yeung, 2018; Engin & Treleaven, 2019; Henman, 2019).

The very word 'algorithm', however, is an ancient one. It is often cited as originated from the 9th century Persian mathematician Al-Khwarizmi, who was influenced by the Indian procedures in mathematics and wrote a book on the art of Hindu reckoning. At face value, an algorithm is nothing more than a set of precise steps to accomplish a designated task that will lead to some desirable outcome. For an algorithm to be considered valid it must have three characteristics: (1) it should be finite; (2) it should have well-defined instructions; and (3) it should be effective. Cooking recipes are algorithms of a sort, since they are a list of instructions to be completed in consecutive order. Yet algorithms are far from trivial. When people say they are worried about the influence of algorithms in their day-to-day lives, they are talking about the application of advanced statistical methods and techniques by private and public organisations to automate decision-making on individual people's access to rights and services and to pick

out patterns and correlations out of enormous data sets in order to make predictions about their behaviour.

Decisions and predictions

It is crucial to understand that a conceptual and analytical distinction must be made between algorithmic decisions and algorithmic predictions, which may or may not exist side by side in organisational contexts. Algorithmic decisions are the digitalised versions of traditional bureaucratic decision-making. They are forms of classification and categorisation most commonly used to automate routinised non-complex administrative decision-making to determine a citizen's or client's status as eligible for rights, services or obligations (Bovens & Zouridis, 2002). Algorithmic prediction, however, is a form of statistical analysis used to identify individuals from a broader group based on specific characteristics or behavioural patterns. Rather than an extension of traditional decision-making, algorithmic prediction is a more recent addition to the tools of government. In itself, algorithmic prediction does not entail an administrative decision, even though this could also be designed into the algorithm. Instead, predictive algorithms are often used to inform human decision-makers about ways to single out people or other targets for tailor-made attention and treatment through risk analysis or behavioural interventions. Canadian criminologist Kelly Hannah-Moffat (2019) speaks of 'psychology informed risk technologies'.

The statistical model underlying algorithmic prediction can be pre-programmed by humans, but may also be 'outsourced' to the algorithm itself through machine learning and artificial intelligence. Although these two terms are often used interchangeably, they are not quite the same thing. Machine learning is a current application of artificial intelligence based around the idea that by giving machines access to data they learn for themselves, without explicit programming, to make accurate predictions. Based on training models, these algorithms, which are not fully pre-designed but adaptive, 'learn' new ways of classification or prediction by analysing large data sets (Binns, 2018). As the name suggests, artificial intelligence carries out tasks in a way that people would consider 'smart'. It is any technology that enables a system to demonstrate human-like intelligence. Artificial intelligence differs from machine learning in that it cannot exist without machine learning – although machine learning can exist without artificial intelligence. Taken together, algorithms, machine learning and artificial intelligence form the new digital infrastructure of our society.

Algorithms and rationalisation

Algorithms can only exist in a stable environment of standardised codes and classifications. They work according to pre-designed 'recipes'. Or, in the case of machine learning, they become autopoietic or self-reproducing (cf. Luhmann, 1990). Data flows silently through the various steps of a recipe unhindered by human interference (Introna & Wood, 2004) – besides the design of the objective function of the algorithm and its data input. Algorithms produce outcomes that do not 'argue'. They do not present an argument or a reasoning, they do not reveal

sources or assumptions, but instead merely construct specific forms of knowledge around things like taste, lifestyle, health and so on, which, in turn, reproduce power. This black box may be opened to make the algorithmic design transparent, but any interference in the functioning of the algorithm is impossible. We consider, therefore, algorithms to be 'instruments of rationalisation' (Peeters & Schuilenburg, 2018) or a 'rationalizing force' (Pasquale, 2015: 15).

By seeing algorithms as similar to bureaucratic or administrative mechanisms rather than to intelligent systems (Caplan & Boyd, 2018: 2), we can better understand the effects they have on the governance of our behaviour in everyday life. Algorithms classify, categorise and process data in organisations in the way forms, procedures and rules do in classic bureaucratic organisations – albeit with a greater speed and a greater amount of data than any human is capable of processing. They are, just like all information technology, characterised by 'simplification' and 'closure' (Kallinikos, 2005). *Simplification* is the process of breaking down a task or problem into a set of operations that needs to be performed sequentially. *Closure*, the necessary complement to simplification, entails 'the isolation and black boxing of the sequential operations, ensuring their execution is protected from external interference' (Cordella & Tempini, 2015: 281). The use of algorithms makes decision-making processes more machine-like. They standardise and formalise tasks in a similar way as the rules and procedures of the classic bureaucracy aimed to do (Gajduschek, 2003).

In two important aspects, however, the analogy between algorithms and bureaucracy falls short. First, algorithms do not leave a paper trail. They are not only less tangible than forms, files and documents, but also less transparent – in both the procedures they follow and in the decisions they make to reach their conclusions. The procedures are designed by IT professionals or adapt themselves through machine learning. The outcomes are produced by a closed system of digital operations. Neither citizens nor the people working with algorithms on a daily basis have insight in or influence on these proceedings. This brings us to a second difference between algorithms and bureaucracies: the exclusion of human agency. As automation becomes more complete, there are ever fewer points of access for people to understand, influence or question the functioning of the system (Eubanks, 2018). Algorithms cannot be held accountable for their actions the way human decision-makers can be. In many cases, decision-makers cannot fully explain how algorithms produce their results. Even if algorithmic outcomes need to be followed up by human decision-making, an organisation that depends on algorithms for its core administrative mechanisms can become a 'digital cage' (Peeters & Widlak, 2018), in which very few people (not even the developers of algorithms) understand how the system works nor the means to influence it.

Algorithmic power

Over the past decade, the power of algorithms has made itself felt in many spheres of society. This suggests that we need to think in terms of algorithms as one of the forms through which power is enacted in our society. Yet, at the same time, an

algorithm's power lies not just in the computer code, but also in the way that it becomes part of 'a code of normalization' (Foucault, 2014: 38). This means that algorithms do not simply have power in the classical sense, as in the sovereign manner of power exertion. Rather, they constitute technologies of government as they provide 'actionable insights' (Ekbia et al., 2015) for techniques that seek to nudge, manipulate or manage behaviour at both the collective and individual level. This means that they do not obstruct, but – instead – provide a 'script' for action (cf. Akrich & Latour, 1992). Or, in the words of Michel Foucault, algorithms 'structure the possible field of action of others' (1982: 221).

To understand this, we should look beyond explanations of algorithms that focus solely on their technological qualities. This means that we should not be preoccupied with the technological question: 'What is an algorithm?' – a question that risks essentialism and functionalism. Instead, we must ask questions involving the functioning of algorithms. How do they work? In which domains? What are their effects on our behaviour? How do governments use them to govern society? By posing these questions one obtains more insight in the specific ways algorithms are deployed in our society. Roughly speaking, we can identify three types of applications: (1) status determination, (2) risk assessment, and (3) population management.

Status determination: algorithms are used to automatically determine someone's status or eligibility for the provision of services or the imposition of duties. Automated tax returns and student grant allocation are two typical examples (Bovens & Zouridis, 2002). This is the most basic type of algorithmic application, which has, in some ways, more to do with classic government – determining rights and obligations – than with contemporary governance. However, in the context of full automation and information architecture, algorithmic status determination can affect the governance of an entire system of public and private organisations. Nowadays, someone's status may be determined by one organisation (for instance, a person's residence status), but this information is used by a potentially infinite number of organisations to determine eligibility for all kinds of services (Peeters & Widlak, 2018).

Risk assessment: algorithms are used to generate automated estimations of probability and risk for the allocation of resources and for the personalised treatment of individuals. Algorithms are used to make operational decisions about the focus of regulatory efforts, of policing, and of fraud detection (Smith & O'Malley, 2017; Yeung, 2018; Engin & Treleaven, 2019), as well as to make decisions regarding the treatment of risky individuals, such as juvenile delinquents (Asquer, 2014; Goel, Rao & Shroff, 2016; Aradau & Blanke, 2017). Risk assessments have enabled actuarial, pre-emptive and preventative forms of governance which try to make 'the future secure and certain' (Schuilenburg, 2015: 67–68).

Population management: algorithms are used to generate behavioural insights on specific target populations for the purpose of actively influencing their future behaviour. In the private sector, customer information is not only used to predict behaviour but also to actively anticipate through personalised offers (Mayer-Schoenberger & Cukier, 2013). The most prominent form of population management in the public sector are 'smart cities', where behavioural insights are used to manage the flow of people in the public domain (Vanolo, 2014; Sadowski & Pasquale, 2015; Morozov & Bria 2018). The smart city implies a way of managing

public space by deploying techniques to profile and actively modify the behaviour of the people in order to stimulate an efficient, safe and consumption-focused use of space (McGuire, 2018; Schuilenburg & Peeters, 2018; Pali & Schuilenburg, 2019).

For a better understanding of algorithmic power, it is necessary to analyse how algorithmic tools reshape power relations between state, private companies, and citizens. Critical theory often frames the politics of data in a trajectory from disciplinary to control societies. In an extension of Deleuze's writings (1990; 2003), numerous authors have tried to conceptualize the power of data. Whether one defines this in terms of 'infopower' (Koopman), 'expository power' (Harcourt), 'datapower' (Chamayou) or 'psycho-power' (Stiegler), it is clear that the embedded nature of algorithms and their potential role in social processes needs to be addressed. This means that we need to think not just about the impact and consequences of algorithms, but also about the powerful ways in which algorithms oscillate in social ordering processes populated by images, legends, stories, symbols, fictions and so on, that are shared by large groups of people, if not the whole society (Ferrell, Hayward & Young, 2015). By exploring the social imaginary of the algorithm, we are, according to David Beer (2017), likely to find broader rationalities, knowledge-making and norms – both in terms of how the algorithm is used to promote certain visions of calculative objectivity and also in relation to the wider governmentalities that this concept can help to open up.

The dark side of algorithmic governance

Every day, we rely on algorithms to make our lives better. The idea is that algorithms are capable of being fairer and more efficient than humans ever could be. Decision-making becomes more reliable, easier, more time-efficient and less costly. However, there are some concerns to be aware of. The ongoing discussion regarding the use of algorithms focuses on the following elements: (1) the eradication of the human factor in decision-making; (2) the focus on efficiency in automated decision-making; and (3) the comprehensiveness of computational analyses (Harcourt, 2007; Christin, Rosenblat & Boyd, 2015; Domingos, 2015; Goel, Rao & Shroff, 2016; Smith, Bennett Moses & Chan, 2017).

First, proponents claim that by eliminating the wicked problem of the human factor, and all the ways it can negatively impact the lives of millions of people, algorithms will make decision-making less prone to bias or sentiments (Sandvig, 2015; Zarsky, 2016). However, critics point out that algorithms often behave in ways that reflect patterns and prejudices that are deeply embedded in society. How do we know we can trust an algorithm's decision? Although algorithms lack the conscious intention to be racist, they can reproduce biases or propagate specific values that reflect the biases of system designers or of input data (Nissenbaum, 2001). For instance, there is a growing concern that 'dirty data' in police practices, created from flawed, racially biased, and unlawful practices, cause discriminatory results, leading to over-policing of high-poverty and non-white urban areas (Richardson, Schultz & Crawford, 2019). This also holds true for algorithmic decision-making based on machine learning. Biased data that reflects unjust socioeconomic inequalities based on education, employment, income or other

attributes may lead algorithms to 'learn' to find new proxies for them (Van Eijk, 2017; Binns, 2018). Models might give a higher risk score to individuals or groups that have been historically more prone to, for instance, defaulting on their loans or being convicted of a crime.

Second, algorithms are able to process a bigger volume of data at a higher velocity than human decision-makers are able to (Laney, 2001). The use of algorithms for risk assessment can also improve efficiency since resources can be allocated more specifically to high-risk areas of control or regulation (Harcourt, 2007). However, critics point out that efficiency comes at a price. First of all, opacity and a lack of transparency are, to a large extent, inherent to algorithms (Grimmelikhuijsen & Meijer, 2014). The reasoning behind the outputs of knowledge-based systems (i.e. systems using predetermined input data and processing procedures) can, in principle, be explained – contrary to machine learning algorithms, which are intrinsically opaque (Danaher, 2016). However, the screen-level bureaucrats who use automatically generated decisions on a daily basis often have no such insight in how algorithms work and produce their results (Peeters & Widlak, 2018). Furthermore, many algorithms are protected by proprietary laws, which further complicate accountability (Pasquale, 2015). In many cases, algorithms have the legal protection of trade secrets and are as closely guarded as the formula for Coca-Cola. Another objection against the efficiency of algorithms are legal concerns regarding privacy and data protection (Polonetsky & Tene, 2013) as well as their compatibility with administrative justice and principles of good governance (Van Eck, 2018). Finally, several authors argue that efficiency for the organisation does not necessarily translate into efficiency or fairness for citizens subjected to automated decisions (Peeters, 2019). Eliminating discretionary space for human decision-making, for instance, complicates the proportional and reasonable treatment of complicated individual cases. In principle, all pathological tendencies of classic bureaucracies also apply to automated decision-making (Peeters & Widlak, 2018).

Third, algorithms are not only able to produce outcomes faster than humans; they are also able to find new patterns and process a number of variables that far exceeds human capacities (Kitchin, 2014). This potential is especially put to use in predictive algorithms (Smith & O'Malley, 2017), which project representations of reality into the future to, for instance, identify crime patterns and suspicious individuals based on data ranging from criminal statistics to the mining of social media (Williams, Burnap & Sloan, 2017). However, comprehensiveness is not the same as accuracy. Critics point out various epistemic concerns. Full prediction is unattainable, since 'universal and perfect surveillance' (Smith, Bennett Moses & Chan, 2017: 267) would be needed to assemble a truly complete data set. Moreover, a theoretical model would always need to be designed into an algorithm to identify the relevant data (ibid.: 268) and prevent them from being lost 'in a fog of possible correlations' (Crawford, 2014). Furthermore, even correct predictions generated by algorithms are based on correlations rather than causal explanations (Mckinlay, 2017), which can complicate the adequate identification of objects of intervention. Besides epistemic complications, critics also warn about the normative

implications of comprehensive algorithmic governance. Algorithms are often used for purposes of control, which leads to concerns about privacy and totalitarian tendencies (Yeung, 2011; Dixon & Gellman, 2014; Edwards, 2016; Bayamlioğlu et al., 2018). Technocratic classifications and codes are by their very nature contested, since they highlight specific elements of a complex reality while ignoring others (Bowker & Star, 2000). The design and use of algorithms, therefore, always implies ethical choices.

Beyond the critique

This book aims to understand the mechanisms and social implications of algorithmic governance. How are algorithmic tools reshaping power relations between state, private companies and citizens? The primary objective is to develop an in-depth analysis of the use of algorithms in our society and the logics, values and assumptions inscribed within it. How can we conceptualise algorithmic governance? What are the dynamics and preconditions that are at its core? We have structured the book around three domains – public administration, criminal justice and smart cities – in order to obtain a deeper understanding of the role of algorithms in our society. Specifically, we aim to make two contributions to the existing research on algorithms.

First, this book brings together three currently dispersed academic discourses: public administration, criminal justice and urban governance. What are the social and organisational consequences of algorithms in the core mechanisms of public authorities, such as decision-making, regulation and service delivery? How do algorithmic applications transform practices of policing and justice? How can we understand the 'smart mentality' of our new cityscapes? Where most studies focus on sectoral applications, the ambition here is to analyse the systemic nature of algorithmic governance and how this translates into new modes of governing society and managing behaviour. While the importance of algorithms has been picked up in various academic debates, this book brings them together into a single conceptual framework. This allows for a full understanding of the importance of algorithms in the governing of society.

Second, this book goes beyond a pragmatic description and offers a constructive critique of algorithmic governance. In many cases, the use of algorithms tends to be self-authorising, running the risk of lacking democratic, moral and juridical legitimacy. However, as algorithmic structures proliferate, it is vital that they are designed and applied in a way that is consistent with the values of social justice, inclusion and solidarity. Our assumption is that algorithms are 'here to stay' and the relevant question, therefore, is how to deal with them. How can we ensure that algorithmic governance is fair and reasonable, just and unbiased? What solutions can be formulated to mitigate the negative effects or implications of algorithmic governance? In short, what could be an ethical and legal framework for the use of algorithms? Each chapter in this book combines critical analysis with a perspective on how we can try to make algorithmic governance compatible with democratic, legal and social values.

Outline of the book

In the first part of the book, the outlines of algorithmic governance are explored in the core mechanisms of public organisations, such as decision-making, regulation, service delivery, and rule enforcement. The contributions in this section conceptualise various aspects of algorithmic governance and explore the way this transforms the governance of society and the internal dynamics of government. Following our editorial introduction, Paul Henman analyses the algorithmic governmentality in the second chapter of this book and argues for instituting greater legal protections and valorising collective modes of being in order to challenge machinic judgement in government. In Chapter 3, Cary Coglianese offers an overview of the main critiques against the use of algorithms in governmental regulation and argues for human capacity building as a means to mitigate them. In Chapter 4, Albert Meijer and Stephan Grimmelikhuijsen raise the question how the use of algorithms may undermine citizens' trust in government and formulate a set of assessment questions to guide public organisations in the implementation of responsible and accountable algorithmic applications. This theme is further developed in the fifth chapter by Arjan Widlak, Marlies van Eck and Rik Peeters in the form of principles of good digital administration to ensure fairness, accountability and proportionality in automated decision-making.

Key aspects of algorithmic justice, such as predictive policing and predictive criminal justice, are conceptualised and analysed in the second part of the book. Predictive policing and predictive justice raise questions about the relation between algorithmic security and values of justice, dignity and solidarity. In the sixth chapter, Fernando Ávila, Kelly Hannah-Moffat and Paula Maurutto argue that it is problematic to assume that the use of machine learning algorithms and big data will lead to more accurate and fairer decisions in criminal justice. The lack of precision and consistency in conceptualisations of fairness and the decontextualised nature of data analysis raise concerns regarding the obfuscation of social values and the discriminatory effects of risk assessment. In Chapter 7, Rosamunde van Brakel proposes to rethink predictive policing in a more empowering, inclusive and democratic way inspired by approaches of democratic technology, digital democracies and positive criminology. Gwen van Eijk discusses the ethical concerns of algorithmic justice in risk-based rehabilitation practices in Chapter 8. She argues that the problem is not in the first place a technological problem, but a problem of human-algorithm interaction, specifically human interpretation of algorithmic prediction and the rationalisation of algorithms.

In the third part of the book, contributions analyse the changing ways our behaviour is governed in public spaces. The focus is on smart cities, the nexus of algorithms and urban governance. In Chapter 9, Marc Schuilenburg and Brunilda Pali look beyond the techno-utopian vision of smart cities and seek to repoliticise the debate by analysing the neoliberal ethos of market-led and technocratic solutions to city governance and development. In Chapter 10, Michael McGuire analyses the way smart cities sponsor an artificial, hygienically controlled urban space. Traditional anxieties about urban spaces are designed out of the smart city and

replaced by a personalised, but ultimately unsubstantial and highly controlled experience of security, wellbeing and connectivity. In Chapter 11, Keith Hayward develops an understanding of what it means to live in an urban space that is ultimately defined and enforced by a computational system. He outlines five putative 'smart city futures' and identifies emerging cultures of resistance to the threat of transitioning from a socio-technical imaginary to a technologically-determined reality.

The concluding chapter, by the editors of this book, draws together the various strands of the arguments of the individual chapters and the guiding theme of the book. The chapter offers five observations on the link between the process of algorithmisation and the governance of society. In an attempt to generalise the most important findings of the chapters, we define the algorithmic society as 'a set of practices and discourses, implicating hybrid connections between governmental and private parties, that is underpinned by a repertoire of relatively new data-driven technologies, which adds new layers to the governance of society through own modes of knowledge, and particular ways of forming new subjects'. We conclude the chapter with directions for new research and further theorising.

References

Akrich, M. and B. Latour. 1992. A summary of a convenient vocabulary for the semiotics of human and nonhuman assemblies. In *Shaping technology/building society: Studies in sociotechnical change*, edited by W. Bijker and J. Law, 259–264. Cambridge, MA: The MIT Press.

Aneesh, A. 2006. *Virtual migration: The programming of globalization*. Durham, NC: Duke University Press.

Aneesh, A. 2009. Global labor: Algocratic modes of organization. *Sociological Theory*, 27 (4): 347–370.

Aradau, C. and T. Blanke. 2017. Governing others: Anomaly and the algorithmic subject of security. *European Journal of International Security*, 3 (1): 1–21.

Asquer, A. 2014. Big data and innovation in the delivery of public services: The case of predictive policing in Kent. In *Handbook of research on democratic strategies and citizen-centered E-Government services*, edited by C. Dolićanin, E. Kajan, D. Randjelović and B. Stojanović, 20–37. Hershey, PA: IGI Global.

Bayamlioğlu, E., I. Baraliuc, L. Janssens and M. Hildebrandt, eds. 2018. *Being profiled: Cogitase ergo sum – 10 years of 'profiling the European citizen'*. Amsterdam: Amsterdam University Press.

Beer, D. 2017. The social power of algorithms. *Information, Communication & Society*, 20 (1): 1–13.

Bennett Moses, L. and J. Chan. 2018. Algorithmic prediction in policing: Assumptions, evaluation, and accountability. *Policing and Society*, 28 (7): 806–822.

Berk, R.A. 2012. *Criminal justice forecasts of risk: A machine learning approach*. New York: Springer.

Berk, R.A. and J. Bleich. 2013. Statistical procedures for forecasting criminal behavior. *Criminology & Public Policy*, 12 (3): 513–544.

Binns, R. 2018. Algorithmic accountability and public reason. *Philosophy & Technology*, 31 (4): 543–556.

Bovens, M. and S. Zouridis. 2002. From street-level to system-level bureaucracies: How information and communication technology is transforming administrative discretion and constitutional control. *Public Administration Review*, 62 (2): 174–184.

Bowker, G.C. and S.L. Star. 2000. *Sorting things out*. Cambridge, MA: The MIT Press.
Caplan, R. and D. Boyd. 2018. Isomorphism through algorithms: Institutional dependencies in the case of Facebook. *Big Data & Society*, doi: 10.1177/2053951718757253, accessed 08-06-2020.
Christin, A., A. Rosenblat and D. Boyd. 2015. Courts and predictive algorithms. *Data & Civil Rights: A New Era of Policing and Justice*. http://www.datacivilrights.org/pubs/2015-1027/WDN-Courts_and_Predictive_Algorithms.pdf; accessed 21-05-2020.
Citron, D. and F. Pasquale. 2014. The scored society: Due process for automated predictions. *Washington Law Review*, 89 (1): 1–33.
Coglianese, C. and D. Lehr. 2017. Regulating by robot: Administrative decision making in the machine-learning era. *The Georgetown Law Journal*, 105: 1147–1223.
Cordella, A. 2010. Information infrastructure: an actor-network perspective. *International Journal of Actor-Network Theory and Technological Innovation*, 2 (1): 27–53.
Cordella, A. and N. Tempini. 2015. E-government and organizational change: Reappraising the role of ICT and bureaucracy in public service delivery. *Government Information Quarterly*, 32 (3): 279–286.
Crawford, K. 2014. The anxieties of big data. *The New Inquiry*, May 30, 2014.
Danaher, J. 2016. The threat of algocracy: reality, resistance and accommodation. *Philosophy & Technology*, 29 (3): 245–268.
Danaher, J., M.J. Hogan, C. Noone, R. Kennedy, A. Behan, A. De Paor, H. Felzmann, et al. 2017. Algorithmic governance: Developing a research agenda through the power of collective intelligence. *Big Data & Society*, doi: 10.1177/2053951717726554; accessed 28-04-2020.
Deleuze, G. 1990. *Pourparlers 1972–1990*. Paris: Minuit.
Deleuze, G. 2003. *Deux régimes de fous: Textes et entretiens, 1975–1995*. Paris: Minuit.
Dixon, P. and R. Gellman. 2014. The scoring of America: How secret consumer scores threaten your privacy and your future. *World Privacy Forum*, April 2, 2014.
Domingos, P. 2015. *The master algorithm: How the quest for ultimate machine learning will remake our world*. New York: Basic Books.
Douglas, T., J. Pugh, I. Singh, J. Savulescu and S. Fazel. 2017. Risk assessment tools in criminal justice and forensic psychiatry: The need for better data. *European Psychiatry*, 42: 134–137.
Edwards, A. 2016. Big data, predictive machines and security: the minority report. In *The Routledge handbook of technology, crime and justice*, edited by M. McGuire and T. Holt, 451–460, London: Routledge.
Ekbia, H., M. Mattiolo, I. Kouper, G. Arave, A. Ghazinejad, R. Suri, A. Tsou, S. Weingart and C.R. Sugimot. 2015. Big data, bigger dilemmas: A critical review. *Advances in Information Science*, 68 (8): 1523–1545.
Engin, Z. and P. Treleaven. 2019. Algorithmic government: Automating public services and supporting civil servants in using data science technologies. *The Computer Journal*, 62 (3): 448–460.
Eubanks, V. 2018. *Automating inequality: How high-tech tools profile, police and punish the poor*. New York: St. Martin's Press.
Ferrell, J., K. Hayward and J. Young 2015. *Cultural criminology: An invitation*. Newbury Park: Sage.
Foucault, M. 1982. The subject and power: afterword. In *Michel Foucault: Beyond structuralism and hermeneutics*, edited by H.L. Dreyfus and P. Rabinow, 208–226. Sussex: Harvester Press.
Foucault, M. 2014. *On the government of the living: Lectures at the collège de France 1979–1980*. Basingstoke: Palgrave Macmillan.

Gajduschek, G. 2003. Bureaucracy: Is it efficient? Is it not? Is that the question? Uncertainty reduction: An ignored element of bureaucratic rationality. *Administration & Society*, 34 (6): 700–723.

Goel, S., J.M. Rao and R. Shroff. 2016. Personalized risk assessments in the criminal justice system. *American Economic Review: Papers & Proceedings*, 106 (5): 119–123.

Grimmelikhuijsen, S.G. and A.J. Meijer. 2014. Effects of transparency on the perceived trustworthiness of a government organization: Evidence from an online experiment. *Journal of Public Administration Research and Theory*, 24 (1): 137–157.

Hamilton, M. 2015. Adventures in risk: Predicting violent and sexual recidivism in sentencing law. *Arizona State Law Journal*, 47 (1): 1–62.

Hannah-Moffat, K. 2019. Algorithmic risk governance: Big data analytics, race and information activism in criminal justice debates. *Theoretical Criminology*, 23 (4): 453–470.

Harcourt, B.E. 2007. *Against prediction: Profiling, policing, and punishing in an actuarial age*. Chicago, IL: Chicago University Press.

Harcourt, B.E. 2015. *Exposed: Desire and disobedience in the digital age*. Cambridge: Harvard University Press.

Henman, P. 2010. *Governing electronically: E-government and the reconfiguration of public administration, policy, and power*. Basingstoke: Palgrave Macmillan.

Henman, P. 2019. Of algorithms, apps and advice: digital social policy and service delivery. *Journal of Asian Public Policy*, 12 (1): 71–89.

Introna, L. and D. Wood. 2004. Picturing algorithmic surveillance: The politics of facial recognition systems. *Surveillance & Society*, 2 (2/3): 177–198.

Kallinikos, J. 2005. The order of technology: Complexity and control in a connected world. *Information and Organization*, 15: 185–202.

Kitchin, R. 2014. *The data revolution: Big data, open data, data infrastructures and their consequences*. London: Sage.

Kleiman, M., B.J. Ostrom and F.L. Cheeman. 2007. Using risk assessment to inform decisions for nonviolent offenders in Virginia. *Crime & Delinquency*, 53 (1): 1–27.

Koopman, C. 2019. *How we became our data: A genealogy of the informational person*, Chicago, IL: The University of Chicago Press.

Landsbergen, D. 2004. Screen level bureaucracy: Databases as public records. *Government Information Quarterly*, 21 (1): 24–50.

Laney, D. 2001. 3D management: Controlling data volume, velocity and variety. https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf; accessed 28-04-2020.

Luhmann, N. 1990. *Essays in self-reference*. New York: Columbia University Press.

Mager, A. 2012. Algorithmic ideology. *Information, Communication & Society*, 15(5): 769–787.

Mayer-Schoenberger, V. and K. Cukier. 2013. *Big data: A revolution that will transform how we life, work, and think*. London: John Murray Publishers.

Mckinlay, S.T. 2017. Evidence, explanation and predictive data modelling. *Philosophy & Technology*, 30 (4): 461–473.

McGuire, M. 2018. Beyond flatland: When smart cities make stupid citizens. *City, Territory and Architecture*, 5 (22): 1–11.

Morozov, E. and F. Bria 2018. *Rethinking the smart city: Democratizing urban technology*. New York: Rosa Luxembourg Stiftung.

Nissenbaum, H. 2001. How computer systems embody values. *Computer*, 34 (3): 118–120.

Olson, D. and K. Subodh. 2010. Enterprise information systems: Contemporary trends and issues. *World Scientific*, 2: 13–16.

Pali, B. and M. Schuilenburg. 2019. Fear and fantasy in the smart city. *Critical Criminology: An International Journal*, doi:10.1007/s10612-019-09447-7; accessed 28-04-2020.

Pasquale, F. 2015. *The black box society: The secret algorithms that control money and information*. Boston: Harvard University Press.

Peeters, R. 2019. The political economy of administrative burdens: A theoretical framework for analyzing the organizational origins of administrative burdens. *Administration & Society*, doi: https://doi.org/10.1177/0095399719854367; accessed 28-04-2020.

Peeters, R. and M. Schuilenburg. 2018. Machine justice: Governing security through the bureaucracy of algorithms. *Information Polity*, 23 (3): 267–280.

Peeters, R. and A. Widlak. 2018. The digital cage: Administrative exclusion through information architecture – The case of the Dutch civil registry's master data management. *Government Information Quarterly*, 35 (2): 175–183.

Perry, W.L., B. McInnis, C.C. Price, S.C. Smith and J.S. Hollywood. 2013. *Predictive policing: The role of crime forecasting in law enforcement operations*. Santa Monica: RAND Corporation.

Polonetsky, J. and O. Tene. 2013. Privacy and big data: Making ends meet. *Stanford Law Review*, 66: 25–33.

Reigeluth, T. 2014. Why data is not enough: Digital traces as control of self and self-control. *Surveillance & Society*, 12 (2): 243–254.

Richardson, R., J. Schultz and K. Crawford 2019. Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. *New York University Law Review Online*, 94 (192): 192–233.

Sadin, E. 2009. *Surveillance global*. Paris: Flammarion-Climats.

Sadowski, J. and F. Pasquale 2015. The spectrum of control: A social theory of the smart city. http://firstmonday.org/ojs/index.php/fm/article/view/5903/4660; accessed 28-08-2020.

Sandvig, C. 2015. Seeing the sort: The aesthetic and industrial defense of 'the algorithm'. *Journal of the New Media Caucus*, 10 (3): 1–21.

Schuilenburg, M. 2015. *The securitization of society: Crime, risk, and social order*. New York: New York University Press.

Schuilenburg, M. and R. Peeters, 2018. Smart cities and the architecture of security: Pastoral power and the scripted design of public space. *City, Territory and Architecture*, 5 (13): 1–9.

Sjöstedt, G. and M. Grann. 2002. Risk assessment: What is being predicted by actuarial prediction instruments?. *International Journal of Forensic Mental Health*, 1 (2): 179–183.

Smith, G.J.D., L. Bennett Moses and J. Chan. 2017. The challenges of doing criminology in the big data era: Towards a digital and data-driven approach. *The British Journal of Criminology*, 57 (2): 259–274.

Smith, G.J.D. and P. O'Malley. 2017. Driving politics: Data-driven governance and resistance. *The British Journal of Criminology*, 57 (2): 275–298.

Van Brakel, R. 2016. Pre-emptive big data surveillance and its (dis)empowering consequences: The case of predictive policing. In *Exploring the boundaries of big data*, edited by B. van der Sloot et al., 117–141. Amsterdam: Amsterdam University Press.

Van der Voort, H.G., A.J. Klievink, M. Arnaboldi & A.J. Meijer. 2019. Rationality and politics of algorithms: Will the promise of big data survive the dynamics of public decision making?. *Government Information Quarterly*, 36 (1): 27–38.

Van Eck, M. 2018. *Geautomatiseerde ketenbesluiten & rechtsbescherming: Een onderzoek naar de praktijk van geautomatiseerde ketenbesluiten over een financieel belang in relatie tot rechtsbescherming (dissertation)*. Tilburg: Tilburg University.

Van Eijk, G. 2017. Socioeconomic marginality in sentencing: The built-in bias in risk assessment tools and the reproduction of social inequality. *Punishment & Society*, 19 (4): 463–481.

Vanolo, A. 2014. Smartmentality: The smart city as disciplinary strategy. *Urban Studies*, 51 (5): 883–898.

Widlak, A. and R. Peeters. 2018. *De digitale kooi: (On)behoorlijk bestuur door informatiearchitectuur – of: hoe we de burger weer centraal zetten in een digitaliserende overheid*. Den Haag: Boom Bestuurskunde.

Williams, M.L., P. Burnap and L. Sloan. 2017. Crime sensing with big data: The affordances and limitations of using open-source communications to estimate crime patterns. *The British Journal of Criminology*, 57 (2): 320–340.

Yeung, K. 2011. Can we employ design-based regulation while avoiding *brave new world*?. *Law, Innovation and Technology*, 3 (1): 1–29.

Yeung, K. 2018. Algorithmic regulation: A critical interrogation. *Regulation & Governance*, 12 (4): 505–523.

Zarsky, T. 2013. Transparent prediction. *University of Illinois Law Review*, 4: 1503–1570.

Zarsky, T. 2016. The trouble with algorithmic decisions: An analytic road map to examine efficiency and fairness in automated and opaque decision making. *Science, Technology and Human Values*, 41 (1): 118–132.

Zuboff, S. 2019. *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York: Public Affairs.