

Responsible and accountable algorithmization

How to generate citizen trust in governmental usage of algorithms

Albert Meijer and Stephan Grimmelikhuijsen

Introduction

Algorithms are increasingly popular in the public sector in countries all around the world: they are used to provide services (Pencheva, Esteve & Mikhaylov, 2018) but also to, for instance, support decision-making (Van der Voort et al., 2019) and predict recidivism (Kleinberg et al., 2017). Furthermore, the police use algorithms to predict crime patterns (Meijer & Wessels, 2019), tax departments use algorithms to detect tax fraud (Zouridis, Van Eck & Bovens, 2020) and local governments use algorithms to make garbage collection more efficient (Ramalho, Rossetti & Cacho, 2017). The current wave of algorithms uses relatively new techniques, such as machine-learning and deep learning, to transform organizational processes (Brynjolfsson & McAfee, 2014; Burrell, 2016).

The ‘magic’ of these new technologies is appealing to governments since they promise to bring us more effective processes, better informed decisions and more insights in complex realities through informative and seamless interfaces. At the same time, the ‘magic’ of these new technologies is also risky since the use of algorithms can produce bias and even discriminatory practices; it can result in errors in the implementation of policies and it can also hamper the interactions between governments and citizens. Therefore, various authors stress that we need to step back and reflect on how algorithms can be applied to realize desirable outcomes (O’Neil, 2016; Eubanks, 2018; Gerards, 2019). For instance, various municipal governments in the Netherlands used a machine-learning algorithm (*Systeem Risicoindicatie, SyRI*) to detect welfare fraud amongst citizens. While at the beginning there was widespread support for this system among government officials, in early 2020 the system was judged ‘discriminatory’ and ‘not transparent’, not only by civil rights activists, but also by the District Court. Vulnerable citizens, often those from a migrant background, were unfairly profiled to be a suspect of welfare fraud.

The example of SyRI in the Netherlands illustrates an issue of wider significance: there is an urgent societal need to not only focus on issues of effectiveness and efficiency but also identify how governments can avoid negative unintended consequences of the use of algorithms – such as bias and problems of fairness – to maintain the trust of citizens (Hoffman, 2019). How can we expect citizens to trust

government if this system works with an algorithm that is both opaque and discriminatory? Various concerns have been raised regarding the impacts of these systems on privacy but also on discrimination of different groups in society and its neglect of human contact. It is still unclear how government organizations will deal with issues such as interpreting big data in a non-discriminatory manner, handling privacy fairly, using means proportional to the objectives and ensuring human contact (Dencik et al., 2019).

We argue that these concerns go beyond the mere implementation of algorithms; they also relate to how organizations transform and change to enable the use of algorithms. In this chapter, we will label this process *algorithmization*: an organization that transforms its working routines around the use of algorithms for its actions and decisions. We highlight that an analysis of algorithmization requires a focus not only on the technology but also on its organizational implementation in terms of the expertise of employees, information resources, organizational structure, organizational policy and monitoring & evaluation to understand why the use of algorithms does or does not produce citizen trust.

In this chapter we link algorithmization to a crucial concept in contemporary governance: *citizen trust in government*. Trust in government is regarded as an essential element in developed societies. It has been found, for example, that if government institutions are not trusted by the citizens they serve, they are unable to function properly (Fukuyama, 1995; Inglehart, 1999; Levi & Stoker, 2000). Given the rapid algorithmization of government, we need to identify desirable forms of algorithmization in the public sector. Two preconditions for maintaining citizen trust have been proposed in the literature: (1) incorporating values in the design of algorithms as a precondition for organizational *responsibility* (e.g. Friedman, Kahn & Borning, 2008; Van den Hoven, 2013) and (2) demonstrating the correct usage of algorithms to the public as a precondition for *accountability* (e.g. Diakopoulos, 2016). In this chapter we argue that algorithmization in the public sector can only sustain citizen trust when it is based on both preconditions.

To this end, we first discuss what we understand by citizen trust and we outline why trust is so important in the public sector. We then offer a discussion of algorithmization as an organizational process and we stress that this organizational process, rather than the technology in itself, demands our attention if we want to strengthen citizen trust. The next sections discuss how two preconditions – responsible and accountable algorithmization – can contribute to citizen trust. We end this chapter by presenting a model for responsible and accountable algorithmization in the public sector.

The fundamental role of trust in government

Although many scholars have emphasized the importance of trust, we start off with a note that trust in government as such is not strictly necessary. People can ‘accept’ and obey an oppressive government, not because they trust it but because they fear the consequences of disobedience. According to political scientist Russell Hardin (1999, 2002), trust in government is ‘only’ needed under relatively benign

circumstances, such as can be found in democratic regimes. Hardin further argues that government functions well as long as it not actively distrusted by people.

A certain degree of trust makes governing much easier and more benign. Many scholars argue that if government is perceived to be trustworthy, citizens tend to comply more often with its demands, laws and regulations without coercion (Tyler, 2006). For instance, Tom Tyler and Peter DeGoey (1996) found that people's evaluations of the trustworthiness of organizational authorities shape their willingness to accept the decisions of authorities and influence their feelings of obligation to follow organizational rules and laws. Indeed, trust can be viewed as an important component of government legitimacy (Tyler, 2006).

Furthermore, Marc Hetherington (1998) highlights the relevance of political trust. Political trust concerns citizens' trust in their political leaders, which translates into more support for politicians and political institutions. This gives leaders more leeway to govern effectively and offers institutions more support and legitimacy. Furthermore, without public support for solutions, problems tend to linger and become more acute; if not resolved, this becomes the foundation for discontent.

Citizen trust is not a necessity, but it is still regarded as highly important for government. But what exactly is trust in government? To better understand citizen trust in government we have to turn to a variety of scholarly disciplines. Understanding why and how people trust has been a central focus of research by psychologists, sociologists, political scientists, economists and organizational scientists (Grimmelikhuijsen, 2012). Across and even within disciplines, countless definitions, concepts and operationalizations are being used. In an attempt to find cross-disciplinary agreement about the concept of trust, Denise Rousseau, Sim Sitkin, Ronald Burt, and Colin Camerer (1998) developed a definition that is frequently cited in the social sciences. According to them, trust is 'a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another'.

According to Rousseau and colleagues, all definitions of trust assume the presence of some form of positive expectation regarding the intentions and behaviour of the object of trust. The object of trust in this chapter is government. An element of this definition that requires more elaboration is 'positive expectations of the intentions or behaviour of another'. Of what, in the context of government, are these positive expectations comprised?

Trustworthiness concerns the characteristics of the object of trust as perceived by an individual (Mayer, Davis & Schoorman, 1995). A large body of literature has attempted to identify specific elements that might influence an individual's perceptions of trustworthy behaviours and intentions (see, for an overview, McKnight, Choudhury & Kacmar, 2002; McEvily & Tortoriello, 2011; Grimmelikhuijsen & Knies, 2017). Generally, the importance of the various elements tends to differ according to the discipline in question, yet some degree of commonality can be found.

The three most commonly cited elements are perceived competence, perceived benevolence and perceived integrity (also sometimes called honesty) (Grimmelikhuijsen, 2012). Perceived competence is the extent to which a citizen

perceives government to be capable, effective, skillful, and professional; perceived benevolence refers to the extent to which a citizen perceives government to care about the welfare of the public and to be motivated to act in the public interest; perceived integrity is whether a citizen perceives government to be sincere, truthful, and to fulfil its promises. It should be noted that benevolence and integrity are of a different nature than competence, as they reflect ethical traits rather than some kind of capability. Benevolence reflects the trustee's motives and is based on altruism. In contrast, competence is a utilitarian dimension of trust, as it refers to the actual functioning of government organizations.

This section discussed the fundamental role of trust in government and how it can be conceptualized. We highlighted that trust should be understood as a multi-dimensional concept that consists of citizens' perceptions of government competence, benevolence and integrity. In the next section, we outline what we mean by algorithmization of government.

Algorithmization in the public sector

Many academic debates focus on the characteristics and features of algorithms as a technological artifact. This perspective focuses on the design of these algorithms to prevent biases and prejudices. We acknowledge the importance of value-sensitive design of algorithms but also stress that it is not only about the design. We know from decades of studies of information and communication technologies in the public sector that we need to study organizational practices to understand the effects of the use of algorithms. This is why we use the term 'algorithmization' as an organizational process rather than algorithm as a technological artifact. Building upon earlier work on informatization in government (Zuurmond, 1994: 42–48), we distinguish the following components of algorithmization:

- 1 *Technology*. The process of algorithmization starts with the introduction of a technology into organizational processes. The algorithm can be a stand-alone decision-support system but also a system that is well integrated in the organization's infrastructure.
- 2 *Expertise*. The use of algorithms in an organization requires a variety of expertise. Experts that know how to work with the system are needed but also experts that maintain the algorithm and ensure that it is properly installed in the organization's information environment.
- 3 *Information relations*. Algorithmic applications will generally build upon existing information in the organization but also produce new types of information. This means that the algorithm has an effect on the information relations within the organization and often also outside of the organization if information from other actors is used.
- 4 *Organizational structure*. The use of algorithms often leads to new collaborations between different departments. Algorithmic applications can also lead to new forms of organizational control if they dictate the implementation of processes.

- 5 *Organizational policy.* Organizations develop policies for the use of an algorithm in the organization. These policies touch upon issues such as the transparency of the algorithm, responsibilities for usage, maintenance, etc.
- 6 *Monitoring and evaluation.* Organizations develop methods and systems for monitoring and evaluating the foreseen and unforeseen outcomes of the use of algorithms in terms of output and effects.

These six elements form the cornerstones of a conceptual understanding of algorithmization and help us to sharpen our perspective when we study how algorithms are used in the public sector. They also provide starting points for thinking about strengthening citizen trust in the use of algorithms. This trust does not only depend on the nature of the technology but also on the experts that guide the use of the algorithm, the information that is used by the algorithm to provide its output, the organizational control over the algorithm, and the policies that organizations have developed to guide the usage and maintenance of the algorithm.

In an empirical study of the Berlin Police, Lukas Lorenz (2019) used this organizational perspective on algorithms to rethink the nature of bureaucratic organizations. Building upon Max Weber's classic work on bureaucratic organizations and Arre Zuurmond's (1998) work on infocratic organizations, Lorenz sketches the contours of a new type of organization: the algocracy. He conceptualizes the algocracy as new ideal type of rational-legal authority that helps to understand and explain how algorithmic systems shape public organizations. He characterizes the algocracy as a further rationalized organizational configuration of the professional bureaucracy rather than of the machine bureaucracy: the standardization of skills is replaced by automated advice.

This discussion highlights that we need to think about the organizational processes surrounding the introduction of new technologies in organizations – the emerging algocratic organizations – to develop ways to strengthen citizen trust in the public sector. To this end, we emphasize two classical approaches to strengthening trust in government organizations: responsibility and accountability.

Responsible algorithmization

A first route for strengthening citizen trust in algorithmization is provided by the notion of responsibility. Responsibility is one of the key concepts in ethical theory and its roots can be traced back to Aristotle. He emphasized that moral responsibility grows out of an ability to reason, an awareness of action and consequences, and a willingness to act free from external compulsion (Roberts, 1989). Responsibility refers to the idea that persons have moral obligations and duties to others, such as their well-being and their health, and to larger ethical and moral traditions such as freedom and empowerment, and that persons, thus, need to consider these obligations and duties in their individual decisions and actions.

More recently, the notion of responsibility has been applied to public organizations. Political scientist Herman van Gunsteren (1976) highlights that we should strive to embed responsibility in (complex) organizations rather than emphasize

the need to control the activities of all individual members of organizations. His approach stresses the need to acknowledge the limitations of bureaucratic control mechanisms such as hierarchy and formal rules and to place more emphasis on the responsibility of individuals in the organization. According to Van Gunsteren, the notion of responsibility is needed when rigid moral norms – embedded in organizational standard procedures – cannot keep up with rapidly changing circumstances and more flexibility is required to apply sound moral judgement. At the same time, this does not mean that ‘anything goes’: judgement needs to be made based on ethically respectable values and reasonable perceptions of relevant facts (Van Gunsteren, 2015: 318). ‘Responsibility forums’ where individual judgement needs to be explained can play a key role in strengthening the responsibility of individuals in organizations.

Furthermore, the notion of responsibility has been used to think about innovation. In the context of the European Union, the notion of responsible innovation has come to play an important role in funding for technology development. The key idea is that innovation traditionally focuses only on gains in efficiency and effectiveness. Other considerations are often regarded as barriers to the innovation process. The notion of responsible innovation reconceptualizes these barriers and stresses that other values need to play a role in the way the innovation process is structured and implemented. In our understanding of responsible algorithmization, we build upon the broader notion of responsible innovation, which Richard Owen, Phil Macnaghten and Jack Stilgoe define as ‘a collective duty of care, first to rethink what we want from innovation and then how we can make its pathways responsive in the face of uncertainty’ (2012: 757–758).

These general notions about responsibility in organizations and responsible innovation can be used as a basis for ideas about the responsible use of algorithms in public organizations. Key elements in this conceptualization are (1) ethical judgement, (2) based on values, (3) and perceptions of relevant facts, (4) to enact a duty of care (5) through responsive pathways. Based on these elements, we formulate the following conceptualization of responsible algorithmization:

Responsible algorithmization refers to the adequate weighing of ethical dilemmas involved in the organizational use of algorithms based on knowledge about the (possible) impacts to ensure that the algorithmization respects moral obligations to others and to moral traditions through methods that are responsive to the various other actors involved.

Responsibility for algorithmization can be operationalized by building upon the notion of value-sensitive design, which can be defined as ‘a theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner throughout the design process’ (Friedman, Kahn & Borning, 2008: 69). For a value-sensitive algorithmization of government, a comprehensive understanding of the values at stake in a specific process of algorithmic decision-making and of how these values are incorporated in the organizational use of the algorithm is needed (Mingers & Walsham, 2010). Thus, we

apply value-sensitivity not only to the design of the technology but also to the other elements of algorithmization (expertise, information resources, organizational structure, organizational policy). The questions that can help guide organizations towards responsible algorithmization are presented in Table 4.1.

How will responsible algorithmization affect citizen trust in government? In the above, we identified value-sensitivity as a core component of responsible algorithmization. This relates directly to the benevolence and integrity dimension of trust in government. Benevolence refers to the expectations by citizens that government is acting benign and in the interest of citizens; integrity refers to expectations of honesty and truthfulness (Mayer, Davis & Schoorman, 1995; Grimmelikhuijsen & Knies, 2017). If algorithmization is done with consideration of relevant values – e.g. algorithms are used in a fair and unbiased manner – this will likely positively affect citizens’ perceptions of the honesty and benevolence of government. Conversely, when citizens, for instance, feel a welfare fraud algorithm targets them unfairly, this is likely to cause a decline in perceived honesty and benevolence.

The different organizational policy components – organizational policy and monitoring & evaluation – are also likely to contribute to citizen trust in government competence. The basic argument here is that well-considered choices in terms of how the algorithm is to be used in the organization and a consistent monitoring and evaluation of the desired and undesired outcomes contribute to

Table 4.1 Assessment questions for value-sensitivity as a precondition for responsible algorithmization

<i>Dimension of algorithmization</i>	<i>Assessment question</i>
Technology	How are the different values at stake identified and embedded in the design of the algorithm?
Expertise	Are the experts that develop, support and maintain the algorithm aware of relevant ethical considerations and can they make value-sensitive choices?
Information relations	Have the value choices in the datasets used by the algorithm been analysed and are the values that follow from new combinations of data acknowledged?
Organizational structure	Has the overall responsibility for a value-sensitive use of the algorithm in organizational practices been clearly allocated?
Organizational policy	Does the organization have a policy for ensuring value-sensitivity in the organizational use of the algorithm?
Monitoring and evaluation	Does the organization have a system for monitoring and evaluating outcomes in terms of the various values at stake in the use of the algorithm?

the perception that government is using these algorithms in a rational manner. There is a reason for caution here, however. If citizens expect governments to perform much better than they actually do, this can also result in a decline of perceived competence (Grimmelikhuijsen, 2012).

In sum, the first condition that we have identified for maintaining the trust of citizens in an organization that uses algorithms is responsible algorithmization. We have argued that value-sensitivity is the basis for responsible algorithmization and we listed six questions that can help organizations assess their level of responsible algorithmization.

Accountable algorithmization

A second route to strengthening citizen trust in algorithmization is provided by the notion of accountability. This notion builds upon the concept of public accountability which political scientist Mark Bovens defines as ‘a relationship between an actor and a forum, in which the actor has an obligation to explain and to justify his or her conduct, the forum can pose questions and pass judgement, and the actor may face consequences’ (2007: 450). Based on this general definition, we can provide a specific definition (see Wieringa, 2020, for an in-depth analysis) of algorithmic accountability:

Accountable algorithmization can be defined as the justification of the organizational usage of an algorithm and explanations for its outcomes to an accountability forum that can ask questions, pass judgement and impose consequences.

Transparency is an important condition for realizing public accountability, although scholars have noted that transparency does not automatically lead to more accountability (Hood, 2010). Albert Meijer (2014) indicates that transparency facilitates accountability if it presents an actual and significant increase in the available information, if there are actors capable of processing the information, and if exposure has a direct or indirect impact on the government or public agency. Without transparency, accountability is difficult to realize since relevant facts that need to be assessed are not available.

Lack of transparency is a key concern regarding the use of algorithms in the public sector (e.g. Lepri et al., 2018). Machine-learning algorithms that use various internal and external data sets are so complicated that the logic of decision-making – and possible biases – are difficult to detect (Janssen & Van den Hoven, 2015). In addition, the lack of transparency may concern the responsibilities, procedures and practices of algorithmic usage in the organization. In response to these concerns, algorithmic transparency has been proposed as a key element of accountable algorithms applications in the public sector (Diakopoulos, 2016; Lepri et al., 2018). We extend this concept to transparency and apply it not only to the algorithm as a technology but also to its organizational use.

The basic idea is that algorithmic decision-making by government should be accessible and explainable (Kroll et al., 2017). Accessibility implies providing clear information about the input, throughput and output of a decision-making process: which data has been used, which decision rules have been applied and what was the outcome? Explainability concerns the substantive reasons for a decision: on what grounds was the decision made and how does this relate to legislation and other formal rules and policies? In short, accountable algorithmization means that algorithmic decision-making needs to be accessible and explainable. Following these considerations, we define a set of questions to guide organizations (see Table 4.2).

Procedural fairness theory offers valuable insights in how transparency – in terms of accessibility and explicability – may affect trust. Procedural justice theory (e.g. Tyler, 2006) posits that individuals can be satisfied with negative decisions as long as they consider the decision procedure to be fair. Accordingly, accessible and explainable algorithmization helps foster fair procedures and eventually more trust in a decision-maker (i.e. government) (Grootelaar & Van den Bos, 2018; Porumbescu & Grimmelikhuijsen, 2018).

Table 4.2 Assessment questions for transparency as a precondition for accountable algorithmization

<i>Dimension of algorithmization</i>	<i>Assessment question for accessibility</i>	<i>Assessment question for explainability</i>
Technology	Is there access to the code to scrutinize design choices?	Does the algorithm provide substantive reasons for decisions or advice?
Expertise	Are the function characteristics of the experts involved in algorithmization transparent?	Are reasons provided for the expertise involved in algorithmization?
Information relations	Is there access to the key features of the data sets used by the algorithm?	Does the organization explain which datasets are used by the algorithm, why and how?
Organizational structure	Are organizational responsibilities for the algorithmization transparent?	Are choices regarding organizational responsibilities for algorithmization explained?
Organizational policy	Is the organizational policy for algorithmization accessible?	Is the organizational policy for algorithmization explained?
Monitoring and evaluation	Is there access to the results of the algorithmization in terms of foreseen and unforeseen effects?	Are the foreseen and unforeseen effects of algorithmization explained?

More specifically, explicability is a core component of procedural fairness. Explaining citizens how an algorithm functions is expected to have a positive impact on levels of trust (cf. Grimmelikhuijsen et al., 2019). A second component of procedural fairness is the neutrality of the decision-maker (Van den Bos, Vermunt & Wilke, 1997). Core elements of Table 4.2, such as the accessibility of datasets, algorithms and organizational policies indicate that, in an optimistic scenario, decisions based on algorithmization are neutral and unbiased. Eventually, similar to value-sensitivity, this relates to how citizens perceive the benevolence and integrity of government.

Transparency regarding the foreseen and unforeseen effects of algorithmization may contribute to the perceived competence of government. If citizens see that algorithmization actually leads to desired outcomes while the undesired outcomes are limited, their trust in government's ability to realize better outcomes may increase. The monitoring and evaluation of algorithmization is also expected to play a key role in contributing to perceived competence.

In sum, the second condition that we have identified for maintaining the trust of citizens in an organization that uses algorithms is accountable algorithmization. Using transparency as a proxy for accountable algorithmization, we have listed 12 questions that organizations can use to assess their level of accountable algorithmization.

Conclusion

In this chapter, we have discussed how 'algorithmization' has become a potent force, changing traditional bureaucracies into algocracies. The new generation of algorithms that are now finding their way to governments across the globe are more than a change of technology: they trigger a range of organizational changes that eventually transform bureaucratic decision-making. In this context, machine-learning algorithms are often portrayed as problematic for accountable and responsible decision-making. We argue that both accountable and responsible algorithmization are needed to sustain citizen trust in the use of these algorithms. The argument we developed in this chapter is summarized in Table 4.3.

The two preconditions of value-sensitivity and transparency are a starting point for realizing responsible and accountable algorithmization. However, this does not resolve all issues. A first issue is that algorithmization is not limited to the use of merely one technological system in an organization. There are entire ecosystems of algorithms that use data from various sources and that are implemented in networks of organizations (Cicirelli et al., 2019). The 'problem of many hands' is compounded by these developments and it is not easy to indicate who is responsible and accountable. In that sense, further work on the assessment questions formulated here is needed to test and re-develop them for ecosystems of algorithms.

A second issue that demands more attention is the fact that machine-learning algorithms change over time. This raises questions about the dynamics of values: value-sensitivity may be ensured at the start but a machine-learning algorithm can, over time, develop patterns that conflict with key values. In addition, transparency

Table 4.3 Potential relations between algorithmization and trust in government

Dimension of trust	Value-sensitivity as a precondition for responsible algorithmization	Transparency as a precondition for accountable algorithmization
Competence	Value-sensitive algorithmization may strengthen perceived competence if the organization demonstrates that various values are measured and its policy focuses on realizing value.	Explicable and accessible monitoring and evaluation of algorithmization provides insights in the outcomes, which is expected to increase perceived competence.
Benevolence	Value-sensitive algorithmization ensures that values important to citizens (e.g. fairness) are not overlooked, which is expected to increase perceived benevolence.	Explicable and accessible algorithmization ensures that government works in the interest of citizens, which is expected to increase perceived benevolence.
Integrity	Value-sensitive algorithmization ensures that decision-makers are more value-sensitive and thus act more ethically; this is expected to increase perceived integrity.	Explicable and accessible algorithmization ensures that external stakeholders have access, which contributes to more open and truthful algorithmization.

may be ensured at the start, but after a process of machine-learning the algorithm can have become opaque because its decision rules have changed following learning processes. This means that the questions formulated here may need to be applied iteratively to ensure that responsibility and accountability persist over time. Further research is needed to provide an understanding of these dynamics of responsible and accountable algorithmization.

In sum, this chapter provides a basic understanding of the importance of responsibility and accountability in producing citizen trust in algorithmization. The key message is that organizations should not only look at designers of algorithms and expect that they will bring the solution: public organizations need to take action to organize responsible and accountable use of algorithms in their organizational processes.

References

- Bovens, M. 2007. Analysing and assessing accountability: A conceptual framework. *European Law Journal*, 13 (4): 447–468. doi: 10.1111/j.1468-0386.2007.00378.x
- Brynjolfsson, E. and A. McAfee. 2014. *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. New York: WW Norton & Company.

- Burrell, J. 2016. How the machine ‘thinks’: Understanding opacity in machine learning algorithms. *Big Data & Society*, 3 (1): 1–12. doi: 10.1177/2053951715622512
- Cicirelli, F., A. Guerrieri, C. Mastroianni, G. Spezzano and A. Vinci. (Eds.). 2019. *The internet of things for smart urban ecosystems*. Cham: Springer.
- Dencik, L., Redden, J., Hintz, A. and H. Warne. 2019. The ‘golden view’: Data-driven governance in the scoring society. *Internet Policy Review*, 8 (2): 1–24. doi: 10.14763/2019.2.1413
- Diakopoulos, N. 2016. Accountability in algorithmic decision making. *Communications of the ACM*, 59 (2): 56–62. doi: 10.1145/2844110
- Eubanks, V. 2018. *Automating inequality: How high-tech tools profile, police, and punish the poor*. New York: St. Martin’s Press.
- Friedman, B., P.H. Kahn and A. Borning. 2008. Value sensitive design and information systems. In *The handbook of information and computer ethics*, edited by K. Himma and H. Trivani, 69–102. New Jersey: John Wiley & Sons Inc.
- Fukuyama, F. 1995. *Trust: The social virtues and the creation of prosperity*. New York: Simon and Schuster.
- Gerards, J. 2019. The fundamental rights challenges of algorithms. *Netherlands Quarterly of Human Rights*, 37 (3): 205–209. doi: 10.1177/0924051919861773
- Grimmelikhuijsen, S. 2012. *Transparency and trust: An experimental study of online disclosure and trust in government*. Doctoral dissertation. Utrecht: University Utrecht.
- Grimmelikhuijsen, S. and E. Knies. 2017. Validating a scale for citizen trust in government organizations. *International Review of Administrative Sciences*, 83 (3): 583–601. doi: 10.1177/0020852315585950
- Grimmelikhuijsen, S., F. Herkes, I. Leistikow, J. Verkroost, F. de Vries and W.G. Zijlstra. 2019. Can decision transparency increase citizen trust in regulatory agencies? Evidence from a representative survey experiment. *Regulation & Governance*. doi: 10.1111/rego.12278
- Grootelaar, H.A. and K. van den Bos. 2018. How litigants in Dutch courtrooms come to trust judges: the role of perceived procedural justice, outcome favorability, and other sociolegal moderators. *Law & Society Review*, 52 (1): 234–268. doi: 10.1111/lasr.12315
- Hardin, R. 1999. Do we want trust in government? In *Democracy and trust*, edited by M.E. Warren, 22–41. Cambridge: Cambridge University Press.
- Hardin, R. 2002. *Trust and trustworthiness*. New York: Russell Sage Foundation.
- Hetherington, M.J. 1998. The political relevance of political trust. *The American Political Science Review*, 92 (4): 791–808. doi: 10.2307/2586304
- Hoffman, A.L. 2019. Where fairness fails: Data algorithms, and the limits of the antidiscrimination discourse. *Information, Communication & Society*, 22 (7): 900–915. doi: 10.1080/1369118X.2019.1573912
- Hood, C. 2010. Accountability and transparency: Siamese twins, matching parts, awkward couple?. *West European Politics*, 33 (5): 989–1009. doi: 10.1080/01402382.2010.486122
- Inglehart, R. 1999. Trust, well-being and democracy. In *Democracy and trust*, edited by M.E. Warren, 88–120. Cambridge: Cambridge University Press.
- Janssen, M. and J. Van den Hoven. 2015. Big and open linked data (BOLD) in government: A challenge to transparency and privacy?. *Government Information Quarterly*, 32 (4): 363–368. doi: 10.1016/j.giq.2015.11.007
- Kleinberg, J., H. Lakkaraju, J. Leskovec, J. Ludwig and S. Mullainathan. 2017. Human decisions and machine predictions. *The Quarterly Journal of Economics*, 133 (1): 237–293. doi: 10.1093/qje/qjx032
- Kroll, J.A., S. Barocas, E.W. Felten, J.R. Reidenberg, D.G. Robinson and H. Yu. 2017. Accountable algorithms. *University of Pennsylvania Law Review*, 165 (3): 633–706.

- Lepri, B., N. Oliver, E. Letouzé, A. Pentland and P.Vinck. 2018. Fair, transparent, and accountable algorithmic decision-making processes. *Philosophy & Technology*, 31 (4): 611–627. doi: 10.1007/s13347-017-0279-x
- Levi, M. and L. Stoker. 2000. Political trust and trustworthiness. *Annual Review of Political Science*, 3: 375–507. doi: 10.1146/annurev.polisci.3.1.475
- Lorenz, L. 2019. *The algocracy: Understanding and explaining how public organizations are shaped by algorithmic systems*. MSc Thesis, Utrecht University.
- Mayer, R., J.H. Davis and F.D. Schoorman. 1995. An integrative model of organizational trust. *Academy of Management Review*, 20 (3): 709–734. doi: 10.5465/amr.1995.9508080335
- McEvily, B. and M. Tortoriello. 2011. Measuring trust in organisational research: Review and recommendations. *Journal of Trust Research*, 1 (1): 23–63. doi: 10.1080/21515581.2011.552424
- McKnight, D.H., V. Choudhury and C. Kacmar. 2002. Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13 (3): 334–359. doi: 10.1287/isre.13.3.334.81
- Meijer, A. 2014. Transparency. In *The Oxford handbook of public accountability*, edited by M. Bovens, R.E. Goodin and T. Schillemans, 507–524. Oxford: Oxford University Press.
- Meijer, A. and M. Wessels. 2019. Predictive policing: Review of benefits and drawbacks. *International Journal of Public Administration*, 42(12):1–9. doi:10.1080/01900692.2019.1575664
- Mingers, J. and G. Walsham. 2010. Toward ethical information systems: the contribution of discourse ethics. *MIS Quarterly*, 34 (4): 833–854. doi: 10.5555.2017496.2917505
- O’Neil, C. 2016. *Weapons of math destruction. How big data increases inequality and threatens democracy*. New York: Crown.
- Owen, R., P. Macnaghten and J. Stilgoe. 2012. Responsible research and innovation: From science in society to science for society, with society. *Science and Public Policy*, 39 (6), 751–760. doi: 10.1093/scipol/scs093
- Pencheva, I., M. Esteve and S.J. Mikhaylov. 2018. Big data and AI: A transformational shift for government: So, what next for research?. *Public Policy and Administration*, 35 (1): 24–44. doi: 10.1177/0952076718780537
- Porumbescu, G.A. and S. Grimmelhuijsen. 2018. Linking decision-making procedures to decision acceptance and citizen voice: Evidence from two studies. *The American Review of Public Administration*, 48 (8): 902–914. doi: 10.1177/0275074017734642
- Ramalho, M.A., R.J. Rossetti and N. Cacho. (2017). *Towards an architecture for smart garbage collection in urban settings*. Presented at the 2017 International Smart Cities Conference (ISC2), Wuxi, September 1–6.
- Roberts, J. 1989. Aristotle on responsibility for action and character. *Ancient Philosophy*, 9 (1): 23–36. doi: 10.5840/ancientphil19899123
- Rousseau, D.M., S.B. Sitkin, R.S. Burt and C. Camerer. 1998. Not so different after all: a cross-discipline view of trust. *Academy of Management Review*, 23 (3): 393–404. doi: 10.5465/amr.1998.926617
- Tyler, T.R. 2006. *Why people obey the law*. Princeton: Princeton University Press.
- Tyler, T.R. and P. DeGoey. 1996. Trust in organizational authorities: The influence of motive attributions on willingness to accept decisions. In *Trust in organizations: Frontiers of theory and research*, edited by R. Kramer and T. Tyler, 331–356. Thousand Oaks, CA: Sage Publications.
- Van den Bos, K., R. Vermunt and H.A. Wilke. 1997. Procedural and distributive justice: What is fair depends more on what comes first than on what comes next. *Journal of Personality and Social Psychology*, 72 (1), 95.

- Van Gunsteren, H.R. 1976. *The quest for control: A critique of the rational-central-rule approach in public affairs*. London: John Wiley & Sons.
- Van Gunsteren, H.R. 2015. The ethical context of bureaucracy and performance analysis. In *The public sector: Challenge for coordination and learning*, edited by F.-X. Kaufmann, chapter 15. Berlin: Walter de Gruyter.
- Van den Hoven, J. 2013. Value sensitive design and responsible innovation. In *Responsible innovation*, edited by R. Owen, J. Bessant and M. Heintz, 75–84. Chichester, UK: Wiley.
- Van der Voort, H.G., A.J. Klievink, M. Arnaboldi and 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. doi: 10.1016/j.giq.2018.10.011
- Wieringa, M. 2020. *What to account for when accounting for algorithms. A systematic literature review on algorithmic accountability*. Paper presented at *ACM Conference on Fairness, Accountability, and Transparency (ACM FAT*)*, Barcelona. ACM, New York, NY, USA, January 27–30.
- Zouridis, S., M. van Eck and M. Bovens. 2020. Automated discretion. In *Discretion and the quest for controlled freedom*, edited by T. Evans and P. Hupe, chapter 20. London: Palgrave Macmillan.
- Zuurmond, A. 1994. *De infocratie. Een theoretische en empirische heroriëntatie op Weber's ideaaltype in het informatietijdperk*. Den Haag: Phaedrus.
- Zuurmond, A. 1998. From bureaucracy to infocracy: Are democratic institutions lagging behind? In: *Public administration in an information age: A handbook*, edited by I.Th.M. Snellen and W.B.H.J. van de Donk, chapter 16. Amsterdam: IOS Press.