University of New South Wales Law Research Series

FROM RULE OF LAW TO STATUTE DRAFTING: LEGAL ISSUES FOR ALGORITHMS IN GOVERNMENT DECISION-MAKING

MONIKA ZALNIERIUTE, LISA BURTON CRAWFORD, JANINA BOUGHEY, LYRIA BENNETT MOSES AND SARAH LOGAN

Forthcoming in Woodrow Barfield (ed), *Cambridge Handbook on the Law of Algorithms* (Cambridge University Press 2019)
[2019] *UNSWLRS* 30

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

This is a draft, pre-edited version, forthcoming in Woodrow Barfield (ed), *Cambridge Handbook on the Law of Algorithms,* Cambridge University Press 2019.

FROM RULE OF LAW TO STATUTE DRAFTING: LEGAL ISSUES FOR ALGORITHMS IN GOVERNMENT DECISION-MAKING

Monika Zalnieriute[*]
Lisa Burton Crawford[**]
Janina Boughey[***]
Lyria Bennett Moses[****]
Sarah Logan[*****]

This is a draft, pre-edited version, forthcoming in Woodrow Barfield (ed), *Cambridge Handbook on the Law of Algorithms,* Cambridge University Press 2019.

Abstract

Governments are increasingly relying on algorithms to automate decision-making in diverse areas, including social welfare, criminal justice, healthcare, law enforcement and national security. This chapter sketches the way in which algorithms are or may be used across the spectrum of government decision making — from the drafting of legislation, to judicial decision making, to the implementation of laws by the executive branch. Then, based on scholarship in the field and our own empirical, doctrinal and theoretical work, the chapter examines the rule of law values affected by automated government decision making systems and the legal and practical issues that the implementation and supervision of such systems may pose in practice.

[*] Research Fellow, Allens Hub for Technology, Law and Innovation, Faculty of Law, UNSW Sydney.
[**] Senior Lecturer and Deputy Director of the Gilbert + Tobin Centre of Public Law, Faculty of Law, UNSW Sydney.
[***] Senior Lecturer, Director, Administrative Law and Justice Project, Gilbert + Tobin Centre of Public Law, Faculty of Law, UNSW Sydney.
[****] Director, Allens Hub for Technology, Law and Innovation, Faculty of Law, UNSW Sydney.
[*****] Lecturer, Department of International Relations, Coral Bell School, College of Asia and the Pacific, The Australian National University, Australia.

TABLE OF CONTENTS

1. Introduction

The (un)limited potential of algorithmic decision making is increasingly embraced by numerous private sector actors, ranging from pharmaceutical to banking, and from transport industries to powerful Internet platforms. The celebratory narratives about the use of big data and machine learning algorithms by private companies to simulate intelligence, improve society and even save humanity are common and widespread. However, the deployment of algorithms to automate decision-making also promises to make governments not only more efficient, but also more accurate and fair. Ranging from welfare and criminal justice, to healthcare, national security and beyond, governments are increasingly relying on algorithms to automate decision-making — a development which has been met with concern by many activists, academics and members of the general public.[1] Yet it remains incredibly difficult to evaluate and measure the nature and impact of automated systems, even as empirical research has demonstrated their potential for bias and individual harm.[2] These opaque and elusive systems often are not subject to the same accountability or oversight mechanisms as other public actors in our legal systems, which raises questions about their compatibility with fundamental principles of public law. It is thus not surprising that numerous scholars are increasingly calling for more attention to be paid to the use of algorithms in government decision-making.[3]

This chapter does not aim to provide an exhaustive analysis of the government use of algorithms. Instead, it, aims to sketch the way in which algorithms are or may be used across the spectrum of government decision making — from the drafting of legislation, to judicial decision making, to the implementation of laws by the executive branch. Then, based on scholarship in the field and our own empirical, doctrinal and theoretical work, the chapter examines the rule of law values affected by automated government decision making systems and the legal and practical issues that the implementation and supervision of such systems may pose in practice.

---

1 See, e.g, Dencik, Lina, et al. "Data scores as Governance: Investigating uses of citizen scoring in public services project report." (2018).

2 Computer scientists are focusing on how such harms occur, how they can be discovered and prevented or lessened computationally, see Zliobaitė, Inde. "Measuring discrimination in algorithmic decision making." *Data Mining and Knowledge Discovery* 31.4 (2017): 1060-1089; Hajian, Sara, Francesco Bonchi, and Carlos Castillo. "Algorithmic bias: From discrimination discovery to fairness-aware data mining." *Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining*. ACM, 2016.

3 Scholars are increasingly calling for more attention to be paid to the governmental context: see, eg, S.J. Mikhaylov, M. Esteve, and A. Campion, 'Artificial Intelligence for the Public Sector: Opportunities and Challenges of Cross-sector Collaboration' (2018) 376(2128) *Philosophical Transactions of the Royal Society A* 20170357 at https://doi.org/10.1098/rsta.2017.0357 (last accessed 10 September 2018); R. Kennedy: 'Algorithms and the Rule of Law' (2017) 17 *Legal Information Management* 170; M. Perry, 'iDecide: Administrative Decision-Making in The Digital World' (2017) 91 *Australian Law Journal* 29.

The remainder of this chapter is divided into two main parts. The first part is primarily descriptive and begins with a discussion of the spectrum of automation and techniques by which it can be achieved (Section 2), before explaining the ways in which automated systems are or may be used in administrative decision-making, including the particularly contentious national security context, judicial decision-making and legislative drafting (Section 3), providing real-life examples of automated systems used in different government-decision making contexts in several different countries. The second part of the chapter then considers the implications of such automation for foundational legal values, and especially the Rule of Law. Section 4 examine the effect of automation on core rule of law values such as transparency, accountability, equality before the law, and coherence and consistency. Section 5 provides a case study of the implications of automation for law enforcement and administrative decision-making in the national security context; this raises many of the same general issues as those raised in the preceding sections, but particularly acutely. Much of the discussion here is focused on the way in which automation may affect foundational public law principles and values as they are understood in Australian law, but given many of these principles and values are shared — at least in general — by other legal systems, the discussion is of broader significance. Finally, Section 6 looks at the question of how governments may (or must) authorize and regulate the use of algorithms in government decision-making.

2. Automation

2.1. Spectrum of Automation

Governments are increasingly relying on algorithms to automate decision-making in diverse areas, including social welfare, criminal justice, healthcare, law enforcement and national security. In these different contexts of decision-making, one can differentiate the levels of automation employed which may vary along the spectrum starting with what is known as 'decision support' (e.g., facial recognition tool helps national security officials make decisions) to 'human-in-the-loop' (e.g., social decisions made with government employee involvement), to the total disappearance of humans from the decision-making process (e.g, national debt collection letters automatically issued without the verification by government officials).[4] These are not separate categories but rather a spectrum moving from fully human decision-making to systems that, while designed by humans, operate largely independent of them.

2.2. Techniques of Automation

4 See, e.g, Rahwan, Iyad. "Society-in-the-loop: programming the algorithmic social contract." *Ethics and Information Technology* 20.1 (2018): 5-14; Sengupta, Sailik, et al. "RADAR—A Proactive Decision Support System for Human-in-the-Loop Planning." *2017 AAAI Fall Symposium Series*. 2017; Cranor, Lorrie F. "A framework for reasoning about the human in the loop." (2008).

Automation inevitably involves different techniques, and sometimes combinations of them. We will focus on two classic types. The first type, sometimes described as the first wave of artificial intelligence ('AI') or expert systems, is a process that follows a series of pre-programmed rules to mirror responses of a human expert in a particular domain.[5] The infamous debt collection programme, known as 'Robo-debt' in Australia and the student welfare provision system in Sweden, discussed later in this Chapter, are contemporary examples of systems that follow a primarily pre-programmed logic. The second category – or 'second wave' of AI – includes techniques such as supervised machine learning and deep learning.[6] These are systems that 'learn' from data (either collected or constructed) so as to draw inferences about new situations. These decisions may be classification (e.g, that an image contains a cat) or predictive (e.g, that an individual is likely to commit a crime in the future). There are a variety of data-driven techniques that can be used so that a system will 'learn' patterns and correlations to generate predictions or reveal insights. Unlike standard statistical methods, machine learning is generally iterative (able to continually 'learn' from new information) and capable of identifying more complex patterns in data. It has been deployed in judicial sentencing and predictive policing in the US, as well as parts of the Social Credit System ('SCS') in China, and in facial recognition systems used in the context of national security, that we will discuss throughout this Chapter.

3. Types of Government Decision-Making

In this chapter, we explore the use of automated systems across the spectrum of government activity, from administrative decision-making, to judicial decision-making, to the drafting of legislation. Government activity in the realm of national security is discussed as a particularly contentious area of administrative decision-making and challenging case study. Even though these contexts may overlap to a certain degree in practice, as is the case, e.g., in China SCS, such preliminary categorization is useful because each context is often subject to different legal frameworks. We briefly introduce these contexts with several examples before discussing the legal implications of deployment of algorithms in these settings in Section 4.

3.1 Administrative Decision-Making

Government officers are responsible for making decisions about an enormous range of issues which directly affect the interests of individuals and businesses. These commonly include decisions about social welfare entitlements, taxation liabilities, licences to

5 See generally A. Tyree, Expert *Systems in Law* (Sydney: Prentice Hall, 1989). R.E. Susskind, *Expert Systems in Law: A Jurisprudential Inquiry* (Oxford: Clarendon Press, 1987) 114–115.

6 J. Launchbury, 'A DARPA Perspective on Artificial Intelligence' (DAPRAtv, YouTube, 2017) at https://www.youtube.com/watch?v=-O01G3tSYpU (last accessed 20 August 2018). The Defence Advanced Research Projects Agency (DARPA) has also named a third wave of artificial intelligence that has not yet been applied to government decision-making and so is not explored further in this paper.

operate businesses, and environmental and planning regulation. While there is great diversity in the topics and legal parameters of government decision-making in these contexts, what they have in common is that they each involve governments applying the law to a specific set of facts. For example, in a licensing context, the government is determining whether or not an individual or business meets relevant eligibility criteria for a licence. Often these decisions involve some degree of discretion.

The use of algorithms to automate administrative government decision-making is not a new phenomenon, it has been deployed in a variety of contexts, such as child protection and provision of social welfare, since the 1980s.[7] More contemporary examples include the use of passport scanners at airports to decide whether a person is entitled to enter into the country, the automatic processing of tax refunds[8] and Australia's controversial welfare debt recovery system—colloquially known as 'Robo-debt'.[9] The 'Robo-debt' system combined data matching , automated assessment through the application of human-authored formulae, and the automated generation of letters to welfare recipients requiring them to provide evidence that they were not overpaid by the government.[10] Another prominent example of the use of algorithms by government is the decision-making of the Swedish National Board of Student Finance (CSN), which manages provision of and repayments for financial aid to students in Sweden.[11] The system, which has attracted attention from scholars,[12] combines data from CSN with publicly available information, including tax information (which is publicly available in Sweden)[13] to fully automate decisions about loan re-payments based on income of the last two years or to

7 Eg J.R. Schuerman et al, 'First Generation Expert Systems in Social Welfare' (1989) 4 *Computers in Human Services* 111; J. Sutcliffe, 'Welfare Benefits Adviser: A Local Government Expert System Application' (1989) 4(6) *Computer Law & Security Review* 22.

8 See information from Australian Taxation Office on the uses of data and analytics at https://www.ato.gov.au/about-ato/managing-the-tax-and-super-system/insight--building-trust-and-confidence/how-we-use-data-and-analytics/.

9 See, generally, Carney,. "The new digital future for welfare: debts without legal proofs or moral authority?'[2018] UNSW Law Journal Forum 1.

10 The data matching itself was not new, but the policy of automatically generating letters requiring individuals to provide evidence that they do not have a debt was introduced as part of a 2015–16 Budget measure, 'Strengthening the Integrity of Welfare Payments' and a December 2015 Mid-Year Economic Fiscal Outlook announcement. It is this policy change, and the large number of people who subsequently received letters requiring them to prove that they were not overpaid that generated public attention and criticism. See Peter Hanks, 'Administrative Law and Welfare Rights: A 40-Year Story from Green v Daniels to "Robot Debt Recovery"' (2017) 89 *AIAL Forum* 1.

11 See the website of the CSN, at https://www.csn.se/languages/english.html (last accessed 6 November 2018). For more on CSN, see Wihlborg, Elin, Hannu Larsson, and Karin Hedström. "" The Computer Says No!"--A Case Study on Automated Decision-Making in Public Authorities." *2016 49th Hawaii International Conference on System Sciences (HICSS)*. IEEE, 2016.

12 Recent literature analysing CSN include: Wihlborg, Elin, Hannu Larsson, and Karin Hedström. "" The Computer Says No!"--A Case Study on Automated Decision-Making in Public Authorities." *2016 49th Hawaii International Conference on System Sciences (HICSS)*. IEEE, 2016.

13 Swedish Tax Agency, 'Taxes in Sweden: An English Summary of Tax Statistical Yearbook of Sweden' (2016) at https://www.skatteverket.se/download/18.361dc8c15312eff6fd1f7cd/1467206001885/taxes-in-sweden-skv104-utgava16.pdf (last accessed 08 March 2019).

support decision-making process (partial automation) in evaluating applications for a reduction in loan-repayments.[14]

Many of the technological tools used by governments are not particularly sophisticated. For example, the data-matching system used to assess welfare debts in Australia was similar to that which had been used for many years to check a person's reported annual tax income against their reported fortnightly income for social security purposes.[15] However, increasingly government agencies around the world are expressing interest and ambition to go beyond the assistance of 'expert systems' and ordinary software used in the past three decades to employing machine learning and predictive analytics in every-day decision-making.[16] The use of these more sophisticated techniques, including machine learning and other predictive analytic techniques, raise additional legal issues related to transparency, accountability and fairness.

3.2. Administrative Decision-Making in the Context of Law Enforcement and National Security

Algorithms and machine learning tools are also increasingly used to automate decision-making in the law enforcement and national security context. Such decisions can be made in an analytic context—concerning whether an individual or a pattern of activity is of relevance to authorities—or in administrative context related to national security, such as immigration. Algorithms and machine learning tools are generally used to help analysts and decision makers make sense of the huge volume of surveillance data available to them. [17]

Contemporary examples of automated decision-making in the context of law enforcement are China's Social Credit System ('SCS') and predictive policing software. The SCS in China (*shehui xinyong tixi*), developed by central government in China and implemented by 43 'demonstration cities' and districts at a local level[18] is a system of

14 E. Wihlborg, H. Larsson, and K. Hedström. '"The Computer Says No!" A Case Study on Automated Decision-Making in Public Authorities' (2016 49th Hawaii International Conference on System Sciences).

15 Senate Standing Committee on Community Affairs, Australian Parliament, Design, scope, cost-benefit analysis, contracts awarded and implementation associated with the Better Management of the Social Welfare System Initiative, 21 June 2017, 2.

16 See, e.g, Dencik, Lina, Arne Hintz, Joanna Redden, and Harry Warne. "Data scores as Governance: Investigating uses of citizen scoring in public services project report." (2018).

17 Bennett Moses, L. De Koker, L. (2017) 'Open Secrets: Balancing Operational Secrecy and Transparency in the Collection and Use of Data by National Security and Law Enforcement Agencies' *Melbourne University Law Review* 4 (12), 530 – 570. Wroe, D. 15/07/18 'Top Officials Golden Rule: In Border Protection, Computer Won't Ever Say no' Sydney Morning Herald https://www.smh.com.au/politics/federal/top-official-s-golden-rule-in-border-protection-computer-won-t-ever-say-no-20180712-p4zr3i.html.

18 A linguistic note made by Rogier Creemers is useful in this context: 'the Mandarin term "credit" (*xinyong*) carries a wider meaning than its English-language counterpart. It not only includes notions of financial ability to service debt, but is cognate with terms for sincerity, honesty, and integrity.' See R. Creemers, 'China's Social Credit System: An Evolving Practice of Control' (2018) at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175792 (last accessed 16 August 2018).

rewards and punishments as feedback to individuals and companies, based not just on the lawfulness, and morality of their actions, covering economic, social and political conduct. [19] Scholars detail how China's SCS combines both traditional pre-programmed system based on points (deducted or adduced based on specific behaviour), and also government cooperation with Chinese tech giant Alibaba in a Sesame Credit system, which relies on an automated assessment of potential borrowers' social network contacts in calculating credit scores.[20] Predictive policing software such as PredPol uses an earthquake prediction model to predict the location of future crimes, using it to make deployment decisions about where police will patrol.[21] The software makes a variety of assumptions, some of which are problematic, and was not subject to rigorous testing and evaluation before adoption.[22] In particular, there are challenges around transparency in the context of operational secrecy and complexity as well as the appropriateness of profiling and discrimination.[23] The use of algorithms in the law enforcement and national security field thus raises context-specific challenges because of the particular legal framework in which national security agencies generally operate and the constraints under which national security policy-making takes place.[24]

3.3. Judicial Decision-Making

Some countries are experimenting with or considering the introduction of algorithms and machine learning tools to automate decision-making by a different branch of the government – the judiciary. Judicial decision-making covers civil and criminal proceedings and, particularly in the context of criminal proceedings, has serious implications for individuals.

While scholars note that the use of algorithms in this area is still at 'their infancy',[25] and have been met with political resistance, there are suggestions that they may be

19 R. Creemers (ed), 'Planning Outline for the Construction of a Social Credit System (2014–2020)' (Eng tr of State Council Notice of 14 June 2014, 25 April 2015) at https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/ (last accessed 16 August 2018).

20 See particularly, R. Creemers, 'China's Social Credit System: An Evolving Practice of Control' (2018) at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175792 (last accessed 16 August 2018); and M. Hvistendahl, 'Inside China's Vast New Experment in Social Ranking' (*Wired*, 14 December 2017) at https://www.wired.com/story/age-of-social-credit/ (last accessed 15 April 2019).

21 See https://www.predpol.com/predicting-crime-predictive-analytics/. Accessed 15 April 2019.

22 Bennett Moses L; Chan J, 2018, 'Algorithmic prediction in policing: assumptions, evaluation, and accountability', Policing and Society, vol. 28, pp. 806 - 822, http://dx.doi.org/10.1080/10439463.2016.1253695, ROS ID: 860882

23 *Ibid.*

24 See, eg, L. Bennett Moses and L. de Koker, 'Open Secrets: Balancing Operational Secrecy and Transparency in the Collection and Use of Data for National Security and Law Enforcement Agencies' (2017) 41 *Melbourne University Law Review* 530; M. Hildebrandt, 'Profiling and the Rule of Law' (2008) 1 *Identity in the Information Society* 55; T. Z. Zarsky, 'Transparent Predictions' [2013] *University of Illinois Law Review* 1503.

25 Sourdin, Tania. "Judge v. Robot: Artificial Intelligence and Judicial Decision-Making." *UNSWLJ* 41 (2018): 1114, at 1115.

increasingly deployed or even transform the judicial system by removing judges altogether.[26] For example, the UK government has proposed a deployment of 'automatic online conviction' process, which has been stalled at the United Kingdom Parliamentary debates since 2017.[27] While this may sound far-fetched, it is in some sense a small extension from existing practices of automating the detection and penalising of speeding and other traffic offences.

One area of judicial decision making where automation tools have already been deployed in practice is the prediction of the likelihood of reoffending in the context of criminal sentencing decisions. For example, in some United States jurisdictions, judges can use automated decision-making tools such as COMPAS ('Correctional Offender Management Profiling for Alternative Sanctions') that draw on historic data to infer which convicted defendants pose the highest risk of re-offending, particularly where there is a risk of violence. Many scholars have expressed concerns that such reliance has been approved by the Conference of US Chief Justices[28] and by the Supreme Court of Wisconsin as well as in various state statutes.[29] In *State v. Loomis* ('*Loomis*'), use of the COMPAS system was held to be permissible on the condition that the decision was not fully delegated to machine learning software and that the judge was notified of the tool's limitations. Thus, a judge will still need to consider a defendant's arguments as to why other factors might impact the risk that they pose. [30] Because judicial sentencing decisions affect the freedom and lives of individuals, the use of algorithms to automate them is particularly controversial.

Beyond concerns in the sentencing context, scholars are increasingly investigating whether machine learning techniques and other AI should play a role in assisting tribunals and judiciary in decision-making, and how that might transform the role of judges in contemporary societies.[31]

---

26 Sourdin, Tania. "Judge v. Robot: Artificial Intelligence and Judicial Decision-Making." *UNSWLJ* 41 (2018): 1114, at 1115.

27 UK Ministry of Justice, 'Transforming Our Justice System: Assisted Digital Strategy, Automatic Online Conviction and Statutory Standard Penalty, and Panel Composition in Tribunals' (Government Response Cm 9391, February 2017).

28 CCJ/COSCA Criminal Justice Committee, 'In Support of the Guiding Principles on Using Risk and Needs Assessment Information in the Sentencing Process' (Resolution 7, adopted 3 August 2011) at http://ccj.ncsc.org/~/media/Microsites/Files/CCJ/Resolutions/08032011-Support-Guiding-Principles-Using-Risk-Needs-Assessment-Information-Sentencing-Process.ashx (last accessed 15 August 2018).

29 See State of Wisconsin v. Loomis, 881 N.W.2d 749 (Wis. 2016). The United States Supreme Court denied certiorari on 26 June 2017. On concerns expressed, see Hannah-Moffat, Kelly. "Algorithmic risk governance: Big data analytics, race and information activism in criminal justice debates." *Theoretical Criminology* (2018): 1362480618763582; Goel, Sharad, et al. "The Accuracy, Equity, and Jurisprudence of Criminal Risk Assessment." *Equity, and Jurisprudence of Criminal Risk Assessment (December 26, 2018)* (2018); Simmons, Ric. "Big Data, Machine Judges, and the Legitimacy of the Criminal Justice System." *UCDL Rev.* 52 (2018): 1067.

30 *Loomis* at [56].

31 See. e.g, Sourdin, Tania. "Judge v. Robot: Artificial Intelligence and Judicial Decision-Making." *UNSWLJ* 41 (2018): 1114; Beatson, Jesse. "AI-Supported Adjudicators: Should Artificial Intelligence Have a Role in Tribunal Adjudication?." *Canadian Journal of Administrative Law & Practice* 31.3 (2018): 307-337.

3.4. Use of Algorithms in Statute Drafting

Another area of government decision-making where automation is anticipated to have a significant impact is legislative drafting. Currently it remains something of a next frontier: while there have been trials of algorithmic tools to assist the drafting of legislation, these have not been widely adopted, and hence the form such tools may take is unclear. Voermans and Verharden have suggested that computerised drafting assistance tools can be categorised as either legislative analysis and review systems, or semi-intelligent drafting-support systems.[32] The former assist legislators to determine the consistency and consequences of legislative drafts. The latter actually assist to translate policy into legislative text, for instance by translating drafting rules and criteria into computer algorithms.[33] Relatedly, there is interest in translating legislation into machine readable code, in order to automate the process of legislative compliance.

At this point, it seems unlikely that human drafters could be completely replaced by AI, given that much of legislative drafting involves the analysis and development of policy before it can be translated into statutory text. However, given advances in the technology used to assist in the drafting of other legal documents—such as contracts[34]—it seems likely that algorithmic tools and machine learning will increasingly play a role in the drafting of legislation.

Scholars are increasingly analysing these challenges, along those arising in judicial and administrative decision-making contexts, by examining how automated decision making in each of the government decision-making contexts complies/compares with the foundational legal values. The following section of this Chapter outlines the main directions and insights of this research and scholarship.

4. The Implications of the Use of Algorithms for Foundational Legal Values and Rule of Law

4.1 Approaches & Conceptual Lenses

Many different conceptual approaches and lenses can be used to ask important questions about the interaction between foundational legal values and the use of algorithms in government decision-making. The research agenda on automation of government decision making is not homogenous and covers many different subjects, approaches, and lenses for analysis. Some scholars see the international human rights framework as part of the foundational legal values and focus on human rights implication of the use of

32 'Leda: A Semi-Intelligent Legislative Drafting Support System' (1993) *Jurix* 81, 81-2.

33 Stijn Debaene, Raf van Kuyck and Bea Van Buggenhout, 'Legislative Technique as Basis of a Legislative Drafting System' (1999) *Jurix* 23, 24.

34 See generally, Kathryn D Betts and Kyle R Jaep, 'The Dawn of Fully Automated Contract Drafting: Machine Learning Breathes New Life into a Decades Old Promise' (2016) 15(1) *Duke Law and Technology Review* 216.

algorithms to automate government decision-making.[35] Often, they focus on privacy and data protection,[36] and increasingly, data-driven discrimination.[37] Related constitutional norms have also been the subject of study in relevant jurisdictions. For example, Ferguson has considered the implications of predictive policing software for a person's right not to be searched without reasonable suspicion in the United States.[38]

Other scholars focus on more abstract legal values. Scholarship on interactions between the foundational legal concepts and norms on the one hand, and automation on the other hand are crystallyzing into a unique research agenda at the intersection of law, philosophy and technology.[39] Some in this field have focused on issues such as the potential and capacity of algorithms and AI to erode traditional legal concerns with prediction and persuasion,[40] or undermine the normative structures and understanding

35 See, e.g, Aust, Helmut Philipp. "Undermining Human Agency and Democratic Infrastructures? The Algorithmic Challenge to The Universal Declaration of Human Rights." *AJIL Unbound* 112 (2018): 334-338.

36 For automation, data protection and privacy, see, e.g, A. Roig, 'Safeguards for the Right Not to be Subject to a Decision Based Solely on Automated Processing (Article 22 GDPR)' (2017) 8(3) *European Journal of Law and Technology* 1; S. Wachter, B. Mittelstadt and L. Floridi, 'Why a Right to Explanation of Automated Decision-Making does not Exist in the General Data Protection Regulation' (2017) 7 *International Data Privacy Law* 76; S. Wachter, B. Mittelstadt and C. Russell, 'Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR' (2017) 31 *Harvard Journal of Law & Technology* 841; I. Mendoza and L. A. Bygrave, 'The Right Not to Be Subject to Automated Decisions Based on Profiling' in T. Synodinou et al (eds), *EU Internet Law: Regulation and Enforcement* (Cham: Springer: 2017); G. Malgieri and G. Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7 *International Data Privacy Law* 243; B. Goodman and S. Flaxman, 'European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"' (2017) 38(3) *AI Magazine* 50.

37 For automation and non-discrmination, see eg, S. Barocas and A. D. Selbst, 'Big Data's Disparate Impact' (2016) 104 *California Law Review* 671; M. B. Zafar et al, 'Fairness Beyond Disparate Treatment & Disparate Impact: Learning Classification without Disparate Mistreatment' (International World Wide Web Conferences Steering Committee, 2017) *Proceedings of the 26th International Conference on World Wide Web* at https://dx.doi.org/10.1145/3038912.3052660 (last accessed 10 September 2018); A. Chouldechova, 'Fair Prediction with Disparate Impact: A Study of Bias in Recidivism Prediction Instruments' (2017) 5 *Big Data* 153; S. Goel et al, 'Combatting Police Discrimination in the Age of Big Data' (2017) 20 *New Criminal Law Review* 181.

38 Andrew Guthrie Ferguson, 'Predictive Policing and Reasonable Suspicion' (2012) 62 *Emory Law Journal* 259,

39 See, eg, recent special issue 'Artificial Intelligence, Technology, and the Law' (2018) 68 supp 1 *University of Toronto Law Journal* 1, focused on law, automation and technology in all sectors of the society. See also K. Yeung, 'Algorithmic Regulation: A Critical Interrogation' (2017) *Regulation & Governance* at https://doi.org/10.1111/rego.12158 (last accessed 10 September 2018); A. Rouvroy and B. Stiegler, 'The Digital Regime of Truth: From the Algorithmic Governmentality to a New Rule of Law' [A. Nony and B. Dillet (tr), 2016] 3 *La Deleuziana* 6 at http://www.ladeleuziana.org/wp-content/uploads/2016/12/Rouvroy-Stiegler_eng.pdf (last accessed 10 September 2018); E. Benvenisti, 'EJIL Foreword – Upholding Democracy Amid the Challenges of New Technology: What Role for the Law of Global Governance?' (2018) 29 *European Journal of International Law* 9.; D. K. Citron and F. Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 *Washington Law Review* 1; M. Hildebrandt and B. Koops, 'The Challenges of Ambient Law and Legal Protection in the Profiling Era' (2010) 73 MLR 428. M. Hildebrandt, 'Profiling and the Rule of Law' (2008) 1 *Identity in the Information Society* 55;.

40 F. Pasquale and G. Cashwell, 'Prediction, Persuasion, and the Jurisprudence of Behaviourism' (2018) 68 supp 1 *University of Toronto Law Journal* 63; F. Pasquale, 'Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Explainability in an Algorithmic Society' (2017) 78 *Ohio State Law Journal* 1243.

of law.[41] Others examined the relationship between data-driven regulation and legal values.[42] Another emerging area of focus in this field is what is referred as 'artificial legal intelligence' and its potential to improve access to justice and to provide benefits for historically discriminated groups.[43]

As this suggests, there are numerous ways to approach the subject that cannot be sufficiently addressed here. Instead, we aim to highlight the core challenges posed by automation to fundamental public law principles and values — including those most iconic legal values, the rule of law.[44] We argue that focus on the rule of law is important because it is a widely accepted standard for measuring the governmental behaviour around the world.[45] Classical works on the rule of law convincingly suggest that it is an ubiquitous and elusive concept, [46] which cannot be accounted fully within the parameters of this Chapter.

In considering the ways in which automation affects the rule of law, it is important not to treat that concept in an 'anatomical' or anachronistic way. As Krygier has long argued, the rule of law is best understood as a goal or ideal; a state in which a legal system is free from certain dangers or pathologies.[47] For many, the rule of law is primarily seen as the antithesis of arbitrary government power. For those seeking clarity as to how to achieve this goal in practice, it is common to look for a list of more concrete criteria. Thus it is often said that the rule of law requires that government action be transparent and accountable, and that all people be treated equally before the law.

While this can yield a useful set of analytical tools, it is important not to lose sight of the fact that these are means to the more important end of non-arbitrariness. Furthermore, there is no definitive 'recipe' for achieving those ends; the means that are appropriate are

41 M. Hildebrandt, 'Law as Computation in the Era of Artificial Legal Intelligence: Speaking Law to the Power of Statistics' (2018) 68 supp 1 *University of Toronto Law Journal* 12; B. Sheppard, 'Warming Up to Inscrutability: How Technology Could Challenge Our Concept of Law' (2018) 68 supp 1 *University of Toronto Law Journal* 36, 37; M. Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Cheltenham: Edward Elgar, 2015).

42 M. Hildebrandt, 'Profiling and the Rule of Law' (2008) 1 *Identity in the Information Society* 55; F. Pasquale, 'Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Explainability in an Algorithmic Society' (2017) 78 *Ohio State Law Journal* 1243; D. K. Citron and F. Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 *Washington Law Review* 1.

43 P. Gowder, 'Transformative Legal Technology and the Rule of Law' (2018) 68 supp 1 *University of Toronto Law Journal* 82.

44 See Monika Zalnieriute, Lyria Bennett Moses and George Williams, 'Rule of Law and Automation in Government Decision-Making,' *Modern Law Review*, Vol. 82(3), https://doi.org/10.1111/1468-2230.12412.

45 See International Congress of Jurists, 'The Rule of Law in a Free Society' (Report of the International Commission of Jurists, New Delhi, 1959), [1].

46 Modern accounts include Lord Bingham, 'The Rule of Law' (2007) 66 CLJ 67, 69. B. Z. Tamanaha, *On the Rule of Law: History, Politics, Theory* (Cambridge: Cambridge University Press, 2004) 2.; P. Gowder, *The Rule of Law in the Real World* (Cambridge: Cambridge University Press, 2016).

47 See especially Martin Krygier, 'The Rule of Law: Legality, Teleology, Sociology' in Gianlugi Palomblla and Neil Walker (ed), Relocating the Rule of Law (Hart Publishing, 2009) 45. For a discussion of how this approach might apply in a particular legal framework, see Lisa Burton Crawford, *The Rule of Law and the Australian Constitution* (Federation Press, 2018).

likely to vary with time, and between jurisdictions. This is particularly pertinent to a discussion of automation. Automation should not be regarded as an inherently suspicious development. The most fruitful way to frame the rule of law question is to ask: can automation help to guard against arbitrary government power, or will it allow it to flourish?

No scholars to date have yet attempted to provide a new account of the rule of law in automated society (this project is still for the future!), but many have examined how automation of government decision-making may affect specific components of the rule of law, such as transparency or accountability.[48] Below we briefly discuss interactions between automation of government decision-making and several of such components: transparency, accountability; equality before the law; and coherence and consistency. [49]

4.2. Automation, Transparency and Accountability

Scholars and policy-makers have noted how automation may offer many potential benefits in enhancing the transparency and accountability of governmental decision-making across different contexts discussed in the Chapter.[50] Put it simply, a system based on pre-programmed rules can inform an affected individual that the reason they were ineligible for a certain benefit was that they did not meet a specific criterion that is a requirement of a particular legislation or operational rule encoded into the logic of the system. However, automation also entails significant challenges to transparency and accountability, that Burrell has convincingly summarized as three 'forms of opacity' of machine learning.[51] Under this frame, first, intentional secrecy may prevent transparency when algorithms are treated as a trade or state secret.[52] For example, in Chinese SCS the details of Sesame Credit system's operation are not clear. While it is known that it relies on behavioural analytics in calculating credit scores,[53] many scholars have argued that individuals have no means to know what information from their social network contacts was used or its precise impact on their scores.[54] Similarly, journalists and scholars have

48 E.g, see De Laat, Paul B. "Algorithmic decision-making based on machine learning from Big Data: Can transparency restore accountability?." *Philosophy & Technology* 31.4 (2018): 525-541.
Ananny, Mike, and Kate Crawford. "Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability." *New Media & Society* 20.3 (2018): 973-989; Singh, Jatinder, et al. "Accountability in the Internet of Things: Systems, law and ways forward." (2018) SSRN, FIND location, where its published.

49 We discuss some of these in detail in Zalnieriute, Bennett Moses and Williams, n 4.

50 For an especially positive account, see C. Coglianese and D. Lehr, 'Regulating by Robot: Administrative Decision Making in the Machine-Learning Era' (2017) 105 *Georgetown Law Journal* 1147.

51 J. Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3(1) *Big Data & Society* 1.

52 J. Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3(1) *Big Data & Society* 1. Pasquale, Frank. *The black box society*. Harvard University Press, 2015.

53 M. Hvistendahl, 'Inside China's Vast New Experment in Social Ranking' *Wired*, 14 December 2017 at https://www.wired.com/story/age-of-social-credit/ (last accessed 10 September 2018).

54 R.ZhongandP.Mozur,'TechGiantsFeeltheSqueezeasXiJinpingTightensHisGrip'*New York Times* (online), 2 May 2018 at https://www.nytimes.com/2018/05/02/technology/china-

pointed that Northpointe Inc (now 'equivant'),[55] which owns the COMPAS tool, has not publicly disclosed its methods in developing the tool used in judicial sentencing, as it considers its algorithms trade secrets.[56] We agree with many scholars that open source software should be favoured in circumstances, where decision-making involves high stakes such as individual liberty.[57]

Burell further notes how technical illiteracy may pose further challenges to transparency and accountability to both expert systems and machine learning, because even if operational information is disclosed, that does not mean that majority of the public will be able to extract useful knowledge from that information.[58] Finally, Burell has suggested that because humans reason differently to machines, they cannot always interpret the interactions among data and algorithms, even if suitably trained. This suggests that the transparency, which is crucial for maintaining/securing the rule of law, may erode over time as machine learning systems become more complex. [59]

4.3. Automation, Accountability and Administrative Justice

The challenges that automation poses for transparency and accountability have been particularly pronounced in the administrative decision-making context. Generally, administrative decision-making by government agencies and employees is subject to constraints of administrative (and sometimes constitutional) law. As noted by US administrative law experts, Coglianese and Lehr, many administrative law principles are built on the assumption that decisions are made by humans, not automated systems.[60] For example, in many jurisdictions, administrative decision-makers are required to provide procedural fairness, or due process, to a person who will be adversely affected by their decision. Decision-makers are also often obliged to provide a statement of reasons for their decisions. The use of machine learning to make administrative decisions thus raises numerous legal issues, as machines may not be capable of complying with administrative law's requirements, such as giving a fair hearing or providing reasons for a decision.[61] Scholars and policy-makers around the world are increasingly paying

xi-jinping-technology-innovation.html (last accessed 10 September 2018).

55 'Equivant' at http://www.equivant.com/ (last accessed 15 April 2019).

56 This is noted in *Loomis* case, at [144]. See generally Pasquale, Frank. *The black box society*. Harvard University Press, 2015.

57 See, e.g., Danielle Keats Citron, 'Technological Due Process' (2008) 85 *Washington University Law Review* 1249; D. K. Citron and F. Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 *Washington Law Review* 1.

58 J. Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3(1) *Big Data & Society* 1, at 4.

59 J. Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3(1) *Big Data & Society* 1, at 10.

60 Coglianese, Cary, and David Lehr. "Regulating by robot: administrative decision making in the machine-learning era." *Geo. LJ* 105 (2016): 1147, at p. 1153.

61 Katie Miller, 'The application of administrative law principles to technology-assisted decision-making' (2016) 86 *AIAL Forum* 20, 27-30

attention to these issues and have adopted a variety of perspectives and approaches.[62] Many have expressed concern about the transparency and accountability challenges raised by the use of algorithm-assisted decision-making in the public sector, and argued that administrative law principles need to be re-framed or adapted for the new algorithmic environment.[63]

Others have argued that the use of algorithms to automate administrative decision-making 'can comfortably fit within these conventional legal parameters.'[64] For example, in a 2004 report, Australia's (now defunct) Administrative Review Council examined the use of automated systems in government decision-making and recommended 27 principles that should be taken into account by governments in designing and delivering automation systems to assist in decision-making. The Council said that '[n]one of the principles put forward is radical or surprising. They are consistent with the best-practice principles generally associated with good administrative decision making'.[65] Had these principles been followed in the design of 'Robo-debt', the worst of its problems would likely have been avoided.

Even so, more fundamental problems may remain. These legal principles reflect a deep-seated view that people whose rights and interests are affected by the state have the right to be treated *as people* — and more particularly, to have their circumstances considered by a human actor who weighs up all the circumstances of their case and decides the best course of action to take. Automation challenges these fundamental ideas of administrative justice.

These ideas were arguably implicit in the decision of the Australian Federal Court in *Pintarich v Federal Commissioner of Taxation.*[66] In brief outline, the Court held that a computer-generated letter ostensibly sent by the Deputy Commissioner of Taxation to a taxpayer advising that a substantial amount of its taxation debt had been excused was not a legally effective 'decision' for the purposes of the *Taxation Administration Act 1953* (Cth). That was so, because a 'decision' necessarily involved a 'mental process' — assumedly undertaken by a human. As a result, the decision ostensibly manifested in the

---

62 Recent analyses of administrative decision-making include: M. Oswald, 'Algorithm-Assisted Decision-Making in the Public Sector: Framing the Issues using Administrative Law Rules Governing Discretionary Power' (2018) 376(2128) *Philosophical Transactions of the Royal Society A* 20170359 at https://doi.org/10.1098/rsta.2017.0359 (last accessed 10 September 2018); C. Coglianese and D. Lehr, 'Regulating by Robot: Administrative Decision Making in the Machine-Learning Era' (2017) 105 *Georgetown Law Journal* 1147; D. Hogan-Doran, 'Computer Says "No": Automation, Algorithms and Artificial Intelligence in Government Decision-Making' (2017) 13 *Judicial Review* 345;

63 Oswald, Marion. "Algorithm-assisted decision-making in the public sector: framing the issues using administrative law rules governing discretionary power." *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376.2128 (2018): 20170359.

64 Coglianese, Cary, and David Lehr. "Regulating by robot: administrative decision making in the machine-learning era." *Geo. LJ* 105 (2016): 1147, at p. 1148.

65 Administrative Review Council, *Automated Assistance in Administrative Decision-Making*, Report No 46, November 2004, vii.

66 [2018] FCAFC 79, esp. [140]. Special leave was sought to appeal this decision to the High Court of Australia, but refused: *Pintarich v Deputy Commissioner of Taxation* [2018] HCASL 322.

letter was not considered to be legally binding, and hence the Deputy Commissioner of Taxation was free to decide again. While this conclusion was framed as one about the meaning of 'decision' in a particular statute, it demonstrates that administrative decision-making is still regarded as an inherently human process, at least within the Australian legal system. In dissent, Kerr J warned that:

> The hitherto expectation that a 'decision' will usually involve human mental processes of reaching a conclusion prior to an outcome being expressed by an overt act is being challenged by automated 'intelligent' decision making systems that rely on algorithms to process applications and make decisions. What was once inconceivable, that a complex decision might be made without any requirement of human mental processes is, for better or worse, rapidly becoming unexceptional. Automated systems are already routinely relied upon by a number of Australian government departments for bulk decision making. … The legal conception of what constitutes a decision cannot be static; it must comprehend that technology has altered how decisions are in fact made and that aspects of, or the entirety of, decision making, can occur independently of human mental input.[67]

At the same time, it is clear that one of the greatest barriers to administrative justice is the size and complexity of the administrative state — and the time and resources that are required to operate it. Automation has the potential to break down or at least diminish these barriers, by increasing the speed and decreasing the cost of administrative decision making. However, the point for present purposes is that any such automation must not only be compatible with administrative law doctrine, but more fundamental public law principles. If automated decision-making continues to be seen as something alien to basic ideas of justice and fairness, it will struggle for acceptance — and encourage challenges and resistance which diminish the efficiency gains it otherwise promises.

4.4. Automation and Equality before the Law

It is widely believed among some governments, private actors and academics that automation can also enhance equality before the law by reducing arbitrariness in the application of law, removing bias and eliminating corruption.[68] However, some legal

---

67 [2018] FCAFC 79, [46]-[49].

68 See, e.g, Srivastava, Shirish C., Thompson SH Teo, and Sarv Devaraj. "You Can't Bribe a Computer: Dealing with the Societal Challenge of Corruption Through ICT." *Mis Quarterly* 40.2 (2016): 511-526. Infante, Davide, and Janna Smirnova. "ENVIRONMENTAL TECHNOLOGY CHOICE IN THE PRESENCE OF CORRUPTION AND THE RULE OF LAW ENFORCEMENT." *Transformations in Business & Economics* 15.1 (2016). Elbahnasawy, Nasr G. "E-government, internet adoption, and corruption: an empirical investigation." *World Development* 57 (2014): 114-126. Shim, Dong Chul, and Tae Ho Eom. "Anticorruption effects of information communication and technology (ICT) and social capital." *International review of administrative sciences* 75.1 (2009): 99-116. Schroth, Peter W., and Preeti Sharma. "Transnational law and technology as potential forces against corruption in Africa." *Management decision* 41.3 (2003): 296-303. Salbu,

researchers argue that it may undermine due process rights and the extent to which people, irrespective of their status, have equal access to rights in the law.[69] For instance, as we explain in our earlier work, the right to review and rectify information in the Australian Robo-debt case was undermined because the debt letter did not explain the importance of the income variation over the year for an accurate calculation of welfare entitlements.[70] By contrast, we pointed out that Sweden's student welfare system provides an explanation of the process involved and a relatively straightforward appeal procedure to challenge the agency's decisions.[71] We further suggested, using the COMPAS example, that with machine learning, lack of transparency is the primary reason why due process rights may be compromised. In particular, lack of transparency in the scoring tool only provides a convicted individual with an opportunity to argue against a score in the absence of any real understanding of the basis for its calculation. Recent scholarship on Chinese SCS demonstrate that similar fairness and equity concerns arise because of lack of transparency in parts of that system.[72]

Finally, scholars from various disciplines and backgrounds have argued that the use of automated decision-making by the governments may further challenge the idea that all individuals irrespective of their status must have equal access to rights in the law and that government should not treat individuals differently due to their demographic group or an immutable trait.[73] As we explain in detail in our earlier research, automation with tools, such as COMPAS and Sesame Credit, can erode this principle because such tools may either explicitly incorporate various static factors or immutable traits, or may incorporate factors such as socio-economic status, employment and education, postal codes, age or gender indirectly, by 'learning' the relevance of variables that correlate with

Steven R. "Information technology in the war against international bribery and corruption: The next frontier of institutional reform." *Harv. J. on Legis.* 38 (2001): 67.

69 See D.L. Kehl, P. Guo and S.A. Kessler 'Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing' Responsive Communities Initiative, Berkman Klein Center for Internet & Society, July 2017) 3 at http://nrs.harvard.edu/urn-3:HUL.InstRepos:33746041 (last accessed 16 August 2018). Danielle Keats Citron, 'Technological Due Process' (2008) 85 *Washington University Law Review* 1249; D. K. Citron and F. Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 *Washington Law Review* 1.

70 Zalnieriute, Bennett Moses and Williams, n 4.

71 As we explain in Zalnieriute, Bennett Moses and Williams, n 4, CSN decisions can be appealed to the National Board of Appeal for Student Aid (Överklagandenämnden för studiestöd, 'OKS'), see OKS website at https://oks.se/ (last accessed 6 November 2018).

72 Creemers, Rogier. "China's Social Credit System: An Evolving Practice of Control." (2018), SSRN; Liang, Fan, et al. "Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure." *Policy & Internet* 10.4 (2018): 415-453; Zalnieriute, Bennett Moses and Williams, n 4.

73 Barocas, Solon, and Andrew D. Selbst. "Big data's disparate impact." *Calif. L. Rev.* 104 (2016): 671. People have particularly strongly objected to courts systematically imposing more severe sentences on defendants who are poor or uneducated or from a certain demographic group: see G. Kleck, 'Racial Discrimination in Criminal Sentencing: A Critical Evaluation of the Evidence with Additional Evidence on the Death Penalty' (1981) 46 *American Sociological Review* 783; L. Wacquant, 'The Penalisation of Poverty and the Rise of Neo-Liberalism' (2001) 9 *European Journal on Criminal Policy and Research* 401; C. Hsieh and M.D. Pugh, 'Poverty, Income Inequality, and Violent Crime: A Meta-Analysis of Recent Aggregate Data Studies' (1993) 18 *Criminal Justice Review* 182.

these.[74] The greatest challenge to the principle of equality before the law thus arises because automation can infer rules from historical patterns and correlation, even when variables, such as race, are not used in machine learning process.[75]

This may occur because many other factors can correlate with, for example, race, including publicly available information, such as, e.g, Facebook 'likes' which are often included as a variable in automated assessments based on social networks.[76] Further problems may arise in judicial decision-making contexts, for instance where a pre-sentencing questionnaire (from which the COMPAS tool draws inferences) records the number of times and the first time a defendant has been 'stopped' by police.[77] O'Neill notes how given historical discriminatory profiling practices by the police in the USA, status of an African-American is likely to correlate with higher numbers and earlier ages in response to this question.[78] Criminologists and legal scholars alike have highlighted how racial differentiation is built into the data from which correlations are deduced and inferences drawn.[79]

4.5. Automation, Complexity and (In)Consistency with the Law

Consistency between government action and the statute book is regarded as a key tenet of the rule of law.[80] A well-designed system of legislation clearly does little to serve the goal of constraining government power if government does not act consistently with it. But consistency can be difficult to achieve, even for the most conscientious government actor, given the complexity of legislation in a modern administrative state and the frequency with which it changes.[81]

---

74 Barocas, Solon, and Andrew D. Selbst. "Big data's disparate impact." *Calif. L. Rev*. 104 (2016): 671. Zalnieriute, Bennett Moses and Williams, n 4.

75 J. Angwin et al, 'Machine Bias' ProPublica, 23 May 2016 at https://www.propublica.org/ article/machine-bias-risk-assessments-in-criminal-sentencing (last accessed 16 August 2018).

76 See especially M. Kosinski, D. Stillwell and T. Graepel, 'Private Traits and Attributes are Predictable from Digital Records of Human Behavior' (2013) 110 *Proceedings of the National Academy of Sciences of the United States of America* 5802 (finding that easily accessible digital records such as Facebook 'likes' can be used to automatically and accurately predict highly sensitive personal information, including sexuality and ethnicity).

77 J. Angwin et al, 'Machine Bias' ProPublica, 23 May 2016 at https://www.propublica.org/ article/machine-bias-risk-assessments-in-criminal-sentencing (last accessed 16 August 2018).

78 C. O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (New York: Broadway Books, 2016) 25–26 ('So if early "involvement" with the police signals recidivism, poor people and racial minorities look far riskier.')

79 See, e.g, Selbst, Andrew D. "Disparate impact in big data policing." *Ga. L. Rev.* 52 (2017): 109. Selbst, Andrew D., and Ferguson, Andrew Guthrie. "Illuminating Black Data Policing." *Ohio St. J. Crim. L.* 15 (2017): 503.

80 See especially Lon Fuller, *The Morality of Law* (Yale University Press, 1962), 81-91.
See further Lisa Burton Crawford, 'The Rule of Law and Human Rights in Australia' in Paula Gerber and Melissa Castan (eds), *Contemporary Perspectives on Human Rights in Australia* (Thomson Reuters, 2019) [forthcoming]. As Crawford explains, legislation at the federal level in Australia is frequently amended. For example, in the period between 2013 and 2017, the *Social Security Act 1991* (Cth) was amended (on average) almost once a month; the *Income Tax Assessment Act 1997* (Cth) was amended every 3.4 weeks.

Policy-makers, business and some scholars have noted how the use of algorithms in government decision-making could improve consistency of government decision-making, and thus make it more consistent with the 'law on the books'.[82] This line of argument is built on the idea that unlike people, pre-programmed systems cannot act with disregard for the rules with which they are programmed. Therefore, researchers have found that automation tools *generally* enhance the consistency of decision-making, even where they are otherwise problematic.[83] As we have argued in our earlier work, the 'social credit system in China works as a tool of social control *because* people can predict the consequences of engaging in particular activities that the government wishes to discourage.'[84] Similarly, Australia's automated debt collection program and Sweden's social welfare system perform the same calculations for everyone, and thus could be said to be 'internally' consistent.

However, many challenges to consistency may arise when the rule that is applied in the pre-programmed system is inconsistent with legal requirements. The inconsistency in such instances arises not because of a differential application of a particular rule in similar cases, but because the application of the rule might differ from its original formulation. A prominent contemporary example of such inconsistency with the law is the Australian Robo-debt programme. While the legality of the government's actions in that context remain unclear, it was clear that many people were advised that there was a discrepancy between their reported income and their legal entitlements when in fact there was not.[85] The problem was not that errors were made – human decision makers make errors too – but rather that errors were made at a far greater rate than would have been the case if the system were entirely human driven. The program had a high error rate because the assumption it made in its calculations—that fortnightly income could be deduced, by averaging, from annual income—did not apply to a significant number of welfare recipients, namely those with variable fortnightly incomes. The letters sent to welfare recipients were also problematic, as they seemed to suggest that the recipient *had* a debt which the recipient needed to *disprove* the existence of, rather than being merely a request for further information. The primary problems with the system were thus ultimately human and occurred in the design process. The data-matching and debt calculation system was designed for the "standard" case where a person's income was the same each week and did not include sufficient measures to deal with people who fell outside that standard case. Its implementation also failed to consider the position of vulnerable people who may not be able to easily access evidence of their income from five or ten years ago, and communication with those affected was poor and proved confusing.

82 For an especially positive scholarly account, see C. Coglianese and D. Lehr, 'Regulating by Robot: Administrative Decision Making in the Machine-Learning Era' (2017) 105 *Georgetown Law Journal* 1147.

83 Zalnieriute, Bennett Moses and Williams, n 4.

84 Zalnieriute, Bennett Moses and Williams, n 4, p.22.

85 Senate Community Affairs References Committee, Parliament of Australia, *Design*, *Scope*, *Cost-Benefit Analysis*, *Contracts Awarded and Implementation Associated with the Better Management of the Social Welfare System Initiative* (2017) at [2.88].

Moreover, the procedures in place to rectify those errors were inadequate. In particular, no humans checked the automated decision to issue individuals with the debt notice, which was presented as a 'fait accompli', with some people not receiving any prior communications because of the errors in address information. [86] The online portal for dealing with debt notices was hard to use,[87] with insufficient human resources to address the concerns or provide information to affected individuals.[88] By contrast, the automated Swedish student welfare system allocates responsibility for decision-making and editing of decisions to humans, with a due process safeguards in place for appealing each decision.[89] This confirms that it is crucial for algorithms to be consistent with the law — and designed and implemented in a way that is sensitive to the legal and social context in which they will operate. It also demonstrates the importance of human oversight of algorithmic decision making to detect inconsistencies that do arise.

One of the primary, contemporary challenges to ensuring that government acts consistently with the law is the complexity of the administrative state. A legislative framework of significant size and complexity is required in order to build and sustain a state of this kind, especially where (as is commonly the case) legislation is the primarily constitutionally prescribed tool by which government can act. But the task of overseeing this legal framework and updating it to ensure it keeps pace with social, economic and scientific developments is one which may strain human capacities. In a healthy legal system, legislation will be harmonious; duplication, overlap, and inconsistency diminishes the accessibility of the law. But when the statute book is large and complex— and in particular, where individual statutes interact with many others — it may be difficult for human drafters to accurately identify the consequences of enacting new, or changing existing, legislation. While many statutes employ similar terms and concepts, it can be difficult for human drafters to keep track of the myriad ways in which they are used across the statute book. Some or all of these tasks could be assisted by automation. Likewise, as Boer, Winkels, Hoekstra and van Engers argue, knowledge management systems may provide a more systematic basis on which legislators can compare legislative proposals with their potential alternatives — and hence to make the best legislative choices.[90]

Yet, there are clear limits on the extent to which legislative drafting can be automated — at least without compromising core legal values or the democratic process. Most democratic theorists stress that the task of deciding when and how to change the law is a complex and sensitive task that must be performed by elected representatives following

86 *ibid* at [3.61].
87 *ibid* at [2.110]
88 *ibid* at [3.98], [3.106], [3.107], [3.119].
89 CSN decisions can be appealed to the National Board of Appeal for Student Aid (Överklagandenämndenförstudiestöd,(OKS)),seeOKSwebsiteathttps://oks.se/(last accessed 19 March 2019).
90 'Knowledge Management for Legislative Drafting in an International Setting' in Daniele Bourcier (ed), *Legal Knowledge and Information Systems* (IOS Press, 1993) 91.

lengthy and careful deliberation in the legislature, and in specialised committees.[91] While algorithms may provide legislators with a clear and accurate source of information to *inform* that deliberation, our conceptions of democracy would demand that legislative choices must in substance be made by those elected to the legislature. In most legal systems, legislative power is explicitly conferred on the legislature, and, while these conferrals may plausibly be read as permitting computer assistance, there would clearly be limits on the extent to which the power may be delegated to non-human actors.[92] The question of whether and how executive power can be delegated to non-human actors is considered further in the next section.

It is also questionable whether and how the myriad principles that inform legislative meaning could be codified. In legal systems such as Australia, legislation is designed with the assistance of an independent office of Parliamentary Counsel with extensive experience and knowledge of the principles and practice of statutory interpretation and design.[93] Legislative drafters and parliamentarians act in light of a rich and largely unstated set of linguistic assumptions, as well as a complex and contested set of interpretive principles set out in legislation and by the courts. The task of reducing these assumptions and principles to code would be challenging to say the least.

5. Exceptionalism, Complexity and Discretion: The National Security Context

Many of legal and practical issues raised by the use of algorithms and machine learning tools in national security context are similar to those raised by the use of such tools in other contexts. Assumptions about accuracy, continuity, the irrelevance of omitted variables and the primary importance of particular sorts of information over others are as relevant to the national security environment as they are to predictive policing and algorithmic accountability in the delivery of social services.[94] However, the use of such tools in decision making in national security raises particular issues.

5.1. Exceptionalism, Privacy and Transparency

Legal exceptionalism is one of the defining features of national security decision making.[95] National security agencies are generally at pains to protect from public scrutiny their methods for acquiring information and the sources via which they acquire

91 See especially Jeremy Waldron, *Law and Disagreement* (Oxford University Press, 1999); Jeremy Waldron, *The Dignity of Legislation* (Cambridge University Press, 2009); Richard Ekins, *The Nature of Legislative Intent* (Oxford University Press, 2013).

92 See for example *Australian Constitution* s 1.

93 Carmel Meiklejohn, *Fitting the Bill: A History of Commonwealth Parliamentary Drafting* (Office of Parliamentary Counsel, 2012).

94 Bennett Moses, L. Chan, J. (2018) 'Algorithmic Prediction in Policing: Assumptions, Evaluation and Accountability' *Policing and Society* 27(7), 806-822. AI Now Institute (2018) Litigating Algorithms: Challenging Government Use of Algorithmic Decision Systems New York.

95 Bennett Moses, L. (2017) Law and Policy Analysis (Report A) *Information sharing and the National Criminal Intelligence System (NCIS)*, section 4. Data to Decisions Cooperative Research Centre.

it. This means national security information regimes are often exempt from privacy and transparency legislation shaping information handling in other policy spaces.

Algorithms and machine learning tools provide particular problems for transparency in the context of national security. In any context, algorithms and machine learning tools contain fundamental opacity to humans,[96] but this opacity is compounded in the national security context by the need to protect sources and methods.[97] This transparency, or the lack thereof, obstructs the possibility of evaluation[98] of the efficacy of automated decision making generated by the use of such tools, and for oversight and accountability more broadly.[99]

With regards to privacy, national security agencies are often exempt from some (though not all) constraints on the collection and use of personal information. Moreover, the use of algorithms and machine learning tools in a national security context can problematise this exceptionalism by destabilising the definition of personal or private information.[100] For example, such tools may be used to interrogate bulk datasets of personal information which may be deidentified at the point of acquisition by national security agencies. But they may be used to match data points and identity trends across bulk dataset which are otherwise deidentified, potentially. This can lead to personal or sensitive information being (re)identified.[101] Managing this risk in the use of automated decision-making, especially in the context of exceptionalism around privacy, requires the implementation of appropriate data governance regimes.[102]

Australian law does not specifically govern agency interrogation of bulk datasets for defence, national security and law enforcement.[103] The US and Canada[104] have rules that govern the bulk analysis and use of personal information in such datasets. In the European Union, the *General Data Protection Regulation* ('GDPR') generally mandates

96 Burrell, J. (2016) 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (3(1) *Big Data and Society*.

97 Bennett Moses, L. De Koker, L. (2017) 'Open Secrets: Balancing Operational Secrecy and Transparency in the Collection and Use of Data by National Security and Law Enforcement Agencies' *Melbourne University Law Review* 4 (12), 530 – 570.

98 Bennett Moses, L. Chan, J. (2018) 'Algorithmic Prediction in Policing: Assumptions, Evaluation and Accountability' *Policing and Society* 27(7), 806-822

99 Bennett Moses, L. De Koker, L. (2017) 'Open Secrets: Balancing Operational Secrecy and Transparency in the Collection and Use of Data by National Security and Law Enforcement Agencies' *Melbourne University Law Review* 4 (12), 530 – 570.

100 For example, in Australia, the Privacy Act 1988 (Cth) applies to the collection and use of 'personal information' and 'sensitive information' by APP entities.

101 Bennett Moses, L. Oboler, A. Logan, S. Wang, M. (2018) *Using 'Open Source' Data and Information for Defence*, *National Security and Law Enforcement.* Data to Decisions Cooperative Research Centre, p31.

102 Bennett Moses, L. et al (Data To Decisions Cooperative Research Centre) (2017) Law and Policy Analysis (Report A) *Information sharing and the National Criminal Intelligence System (NCIS)*, section 4. .

103 An exception is the Data Matching Program (Assistance and Tax Act) 1990.

104 Bennett Moses, L. Oboler, A. Logan, S. Wang, M. (2018) *Using 'Open Source' Data and Information for Defence*, *National Security and Law Enforcement.* Data to Decisions Cooperative Research Centre , section 2.3.6.

that data subjects receive meaningful, if limited, information about the logic involved in processing of their information by automated systems, as well as the significance and the envisaged consequences of automated decision-making systems. [105] However, decision-making in the context of defence, national security, and law enforcement, is exempted and such a right does not apply in the contexts.[106] National legislation in EU Member States, which complements the GDPR and implement the Law Enforcement Directive also entail such exceptions, because national security is not within EU' competence and belongs to the national governments. For instance, the United Kingdom's *Data Protection Act 2018* includes restrictions on automated decision-making, spelling out the notification and appeal requirements for such processing when it is authorized by law.[107] However, just like the GDPR, the UK Act provides for exemptions for data processing in the context of law enforcement and national security.

5.2. Access to Tools and Data

Interrogation of bulk datasets using algorithms and machine learning techniques is a complex, highly specialised task. Governments are often unable to design or implement such tools themselves, lacking the human or technical capacity. Analytic services providers can step in to fill this breach, analysing data themselves or designing tools to do so, including in the national security sector. However, the use of such firms raises important issues, and their obligations may not be clear in emerging governance regimes. For example, in the national security sector, such corporate actors may have access to sensitive and/or personal data, including across datasets, raising issues of privacy as above. And additional issues may arise concerning the right to control and reuse derived data in this context.[108]

The role of corporate actors and their impact on access to and analysis of data is particularly pertinent in the context of open source intelligence, which has become an increasingly important tool of national security policymaking, and one substantially driven by algorithms and machine learning tools because of the sheer bulk of information

105 Articles 13-15 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.

106 Article 23 GDPR. The processing of personal data for law enforcement purposes is dealt with in a separate instrument, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016, L.119/89. Member States are also offered a derogation allowing legacy processing systems to remain in place until 6th May 2023, with the option of a three-year extension to 2026, where there is a "disproportionate effort" required to bring them into compliance.

107 S 14 of UK Data Protection Act 2018.

108 L Bennett Moses. A Maurushat, S Logan, (2017) Law and Policy Analysis (Report A) *Information sharing and the National Criminal Intelligence System (NCIS)*, section 4. Data to Decisions Cooperative Research Centre, section 4. pp10-11.

available for analysis.[109] Open source intelligence is information used for intelligence purposes which is publicly available rather than being obtained by covert means, as is usually the case in intelligence. Social media feeds, real estate information, some commercial website data, newspapers and some browsing information are all potentially examples of open source intelligence. Policymakers and analysts use algorithms and machine learning tools to automate the collection and analysis of these large volumes of information for analysts and, in some cases, automated decision-making systems.[110]

However, even though national security agencies may have access to tools, laws and regulations which allow them to analyse this sort of data, they may not be able to access it easily or even at all. Corporate actors generally seek to protect their data from being accessed, especially by algorithms and machine learning tools held by or used in support of national security and law enforcement agencies.[111] This is because data in this context is not only a commercial asset and protected as such, but also because companies seek to protect their customer's privacy from national security and law enforcement agencies.[112] Companies bar developers from designing algorithmic and machine learning tools to facilitate agency access to their information, and have repeatedly disbarred data brokers which access their API to provide access to national security and law enforcement agencies for surveillance purposes. Barred from accessing the data directly, some agencies may buy bulk social media data from data brokers for analytic purposes, to understand trends in social activity and also to create and train analytic tools.

The legal context for automated collection and analysis of open source intelligence is often unclear. Internationally, case law in the area of web scraping more broadly is in a state of evolution, and has largely focused on copyright principles as a way of asserting ownership over data which has been scraped.[113] For example, if an agency buys bulk social media data to train analytic tools, the latter activity involves replicating copyrightable material, then this would *prima facie* involve copyright infringement, allowing the original copyright holder to assert their rights over a state agency which may have scraped that information. While there is an exception for the temporary

109 See, for example, S Mateescu et al, 'Social Media and Law Enforcement', *Data and Civil Rights* Conference 2015; B van der Sloot & S van Schendel 'Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study' (2016) 7 *Journal of Intellectual Property, Information Technology and E-Commerce Law*.

110 S Logan, J Chan, J. (2018) *Using 'Open Source' Data and Information for Defence, National Security and Law Enforcement. Interview Report for Research Question 3 (Report B)* Data to Decisions Cooperative Research Centre, p6

111 Although note arguably only in the case of Western democracies.

112 S Logan, J Chan, J. (2018) *Using 'Open Source' Data and Information for Defence, National Security and Law Enforcement. Interview Report for Research Question 3 (Report B)* Data to Decisions Cooperative Research Centre, p. 7 – 12.

113 Ryanair Ltd v PR Aviation BV [2015] EUECJ (Case C-30/14) [45] The case, however, highlights that, in the EU, contractual terms which prevent scraping may be invalid if the data is subject to copyright or a 'Sui generis right' and the scraping could be considered normal use, as the Gerechtshof te Amsterdam (Court of Appeal, Amsterdam) found in an earlier hearing on the case

reproduction of works as a necessary part of a technical process in countries like Australia,[114] this probably does not apply to data mining.[115]

Web scraping for national security purposes is not subject to specific legislation in Australia.[116] In the US, the *Computer Fraud and Abuse Act 1986* makes it an offence to obtain 'information from any protected computer' if one 'intentionally accesses a computer without authorization or exceeds authorized access'.[117] A preliminary ruling in the on-going case of *hiQ Labs, Inc. v. LinkedIn Corp.*, however, found that a 'user does not 'access' a computer 'without authorization' by using bots when the data it accesses is otherwise open to the public'.[118] In doing so, the ruling differentiates between 'public data' and data that required a login.[119] The ongoing case is considered to have significant implications for control of data and the legality of different forms of data scraping.[120] While web scraping for the purposes of profiling is explicitly regulated in the EU's General Data Protection Regulation (GDPR), however, the usual a national security exemption applies.[121]

And even within government access to information for analysis via big data techniques is not always clear. Information sharing between government national security agencies is often limited, beset by problems of governance, legislation, technology and organisational culture.[122] As the example of open source intelligence indicates, automation of data processing is becoming increasingly important as a tool for national security and law enforcement agencies. However, the legality of particular practices, and access to data itself, is sometimes unclear and will depend on contractual terms with private sector platforms and data brokers, as well as (to the extent they apply to relevant agencies) copyright law, privacy law, computer offences and more specific governance of agency practices.

In the final section of this Chapter we take a brief look at the regulatory directions focusing on the use of algorithms in government decision-making.

---

114 Copyright Act s 48B.

115 ALRC, '*Copyright and the Digital Economy*' (Discussion Paper No 79, ALRC, 5 June 2013) 164.

116 Web scraping is not expressly regulated through legislation in Australia and there is no case law.. . (B4) legal report p15)

117 18 U.S.C. § 1030(a)(2)(C)

118 hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1109, 1112—1113 (ND Cal, 2017) 1113

119 Ibid 1110, 1119.

120 Tony Hughes, 'Moody's Analytics Economist: Why the LinkedIn Data Case Is a Lose-Lose Situation', Fortune.com, 16 March 2018 < http://fortune.com/2018/03/16/linkedin-hiq-labs-data-case/>; Casey Fiesler, 'Law & Ethics of Scraping: What HiQ v LinkedIn Could Mean for Researchers Violating TOS', Medium, 15 August 2017 <https://medium.com/@cfiesler/law-ethics-of-scraping-what-hiq-v-linkedin-could-mean-for-researchers-violating-tos-787bd3322540> Bennett Moses, L. Oboler, A. Logan, S. Wang, M. (2018) *Using 'Open Source' Data and Information for Defence, National Security and Law Enforcement.* Data to Decisions Cooperative Research Centre.

121 Article 23, General Data Protection Regulation

122 L Bennett Moses, A Maurushat, S Logan (2017) Law and Policy Analysis (Report A) *Information sharing and the National Criminal Intelligence System (NCIS),*

6. Regulatory Directions of Government Use of Algorithms

6.1. When is Automation of Government Decision-Making Authorized?

Legislation (at least in Australia), generally confers power on a specific (human) decision-maker, such as a Minister or other executive office holder. The use of algorithms to *assist* the human decision-maker generally does not require specific statutory authorisation—but the human (or their lawful delegate) remains legally responsible for the decision. Government departments and agencies are generally authorised to make acquisitions, including of computer software, in compliance with relevant procurement policies and procedures.[123] However, where the machine *itself* makes the 'decision', then legal issues may arise, as demonstrated by the case of *Pintarich* discussed above. Here, the Federal Court of Australia found in 2018 that an automated 'decision' was not a 'decision' for the purposes of judicial review, because no 'mental process' was involved in reaching it.[124] This meant that the Australian Taxation Office was not bound by the automated 'decision' and could later demand a higher sum from the taxpayer.

Some legislation specifically authorises the use of software within the decision-making system otherwise established by legislation. For example, in Australia, there are at least 29 Commonwealth Acts and instruments that specifically authorise automated decision-making.[125] To illustrate, section 6A of the *Social Security (Administration) Act* provides that "The Secretary may arrange for the use, under the Secretary's control, of computer programs for any purposes for which the Secretary may make decisions under social

123 For these policies and procedures in Australian law see: Nicholas Seddon, *Government Contracts: Federal, State and Local* (Federation Press, 2018).

124 *Pintarich v Deputy Commissioner of Taxation* [2018] FCAFC 79.

125 *Social Security (Administration) Act 1999* (Cth) s 6A; *A New Tax System (Family Assistance) (Administration) Act (Cth)* s 223; *Migration Act 1958* s 495A; *Australian Citizenship Act 2007* (Cth) s 48; *Superannuation (Government Co-contribution for Low Income Earners) Act 2003* s48*; National Consumer Credit Protection Act 2009* (Cth) s 242; *Paid Parental Leave Act 2010* (Cth) s 305; *Carbon Credits (Carbon Farming Initiative) Act 2011* (Cth) s 287; *Australian National Registry of Emissions Units Act 2011* (Cth) s 87; *Business Names Registration Act 2011* (Cth) s 66; *My Health Records Act 2012* (Cth) s 13A; *Child Support (Assessment) Act 1989* s 12A; *Child Support (Registration and Collection) Act 1988* (Cth) s 4A; *Australian Education Act 2013* (Cth) s 124; *Trade Support Loans Act 2014* (Cth) s 102; *Customs Act 1901* (Cth) s 126H; *Biosecurity Act 2015* (Cth) s 280(6), (7); *Export Control Act 1982* (Cth) s 23A(2)(h); *Aged Care Act 1997* (Cth) s 23B.4; *VET Student Loans Act 2016* (Cth) s 105; *National Health Act 1953* (Cth) s 101B; *Military Rehabilitation and Compensation Act 2004* (Cth) s 4A; *Safety, Rehabilitation and Compensation (Defence-Related Claims) Act 1988* (Cth) s 3A; *Veterans' Entitlements Act 1986* (Cth) s 4B; *Therapeutic Goods Act 1989* (Cth) s 7C(1); *Export Control (High Quality Beef Export to the European Union Tariff Rate Quotas) Order 2016* cl 42*; Export Control (Sheepmeat and Goatmeat Export to the European Union Tariff Rate Quotas) Order 2016* cl 25; *Export Control (Beef Export to the USA Tariff Rate Quota) Order 2016* cl 19A; *Export Control (Dairy Produce Tariff Rate Quotas) Order 2016* cl 36; E*xport Control (Japan-Australia Economic Partnership Agreement Tariff Rate Quotas) Order 2016* cl 19. These were identified in Simon Elvery, 'How algorithms make important government decisions – and how that affects you' *ABC News* (21 July 2017), http://www.abc.net.au/news/2017-07-21/algorithms-can-make-decisions-on-behalf-of-federal-ministers/8704858 and Hon Justice Melissa Perry, 'iDecide: Administrative Decision-Making in the Digital World' (2017) 91 *Australian Law Journal* 29, 31.

security law." There is also an Australian law that authorises some data matching, which is often a step taken as preliminary to automated decision-making.[126]

There are important questions to ask about legislative provisions that specifically authorise the use of automation, including:

- What requirements exist for auditing, testing and evaluation, as well as the frequency and nature of these;
- Whether there is oversight in relation to the purchasing or use of particular software and systems;
- Whether there are procedures by which the proper functioning of systems can be challenged by affected parties;
- Whether there are procedures for challenging specific decisions where they are based on inaccurate data or falsely matched data, lead to an erroneous conclusion, or are biased (for example, because they have a disparate impact on a particular group[127]);
- Whether there are due process or procedural fairness protections for individuals affected by a decision.[128]

To address these important questions and concerns, the idea of regulating automated decision-making, is increasingly being considered by various governments around the world.

6.2. Regulation of Automated Decision-Making

6.2.1. Limited Governmental Regulation

Regulation of automation of decision-making is increasingly seen as necessary to ensure that particular standards or procedures are complied with when decision-making is fully or partially automated. For example, in the UK, there has been a call for increased transparency concerning the use of algorithms by government and the appointment of a "ministerial champion" to provide oversight of such use.[129] A Centre for Data Ethics and Innovation has been launched.[130]

126 *Data Matching Program (Assistance and Tax) Act 1990*.

127 See Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact' (2016) 104 *California Law Review* 671

128 See generally Kate Crawford and Jason Schultz, 'Big Data and Due Process: Towards a Framework to Redress Predictive Privacy Harms' (2014) 55 *Boston College Law Review* 93; Danielle Keats Citron, 'Technological Due
Process' (2008) 85 *Washington University Law Review* 1249.

129 House of Commons Science and Technology Committee, *Algorithms in Decision-Making*, Fourth Report of Session 2017-19 (15 May 2018) 3.

130 Information on the Centre is available on its website at https://www.gov.uk/government/groups/centre-for-data-ethics-and-innovation-cdei.

However, such initiatives are often at their early stages, are still relatively rare. The existing regulation of automation of decision-making (if any) most often operates as part of the broader set of rules relating to the use and processing of personal information, commonly referred to as data privacy laws. Most influential of such provisions can be found in the EU *General Data Protection Regulation* ('GDPR').[131] As was briefly mentioned in the previous section of this Chapter, Article 15(1)(h) of the GDPR articulates the right for any individual subject to automated decision-making, including profiling, to obtain "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject." Article 22(1) of the GDPR further states:

> *The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.*

The 'right not be subjected to a decision based solely on automated processing' is however subject to explicit exceptions, which relate to contracts, explicit consent, and data uses authorised by law, including in the context of national security and law enforcement.[132] The effectiveness of this provision in regulating and/or limiting the automation of decision-making in practice is further impaired by the fact that the provision only applies to a *fully* – and not *partially* - automated decisions. Some academic commentary on the scope of these GDPR provisions thus suggests their likely limited role in changing the decision-making practice.[133] Similar conclusion on the importance of the degree of automation involved in decision-making was reached in the US case of *State v Loomis*, where such comparable due process right to be informed of the logic behind COMPAS scoring tool was found not to apply to decisions that only rely partially on the output of an automated process.

6.2.2. Voluntary Regulatory Initiatives

Beyond currently limited governmental regulation, a variety of voluntary standards, principles and guidelines have been or are being developed by various private and informal bodies. Many of these initiatives focus on categories that may intersect with rather than coincide with the use of automation in government decision-making. For example, there are projects within the Artificial Intelligence, Ethics and Society (AIES) conference,[134] the IEEE's (Institute of Electrical and Electronics Engineers) Global

131 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.

132 Article 22(2) of the GDPR.

133 Eg Lilian Edwards & Michael Veale, 'Slave to the Algorithm? Why a 'Right to an Explanation' is Probably Not the Remedy you are Looking For' (2017) 16 *Duke Law and Technology Review* 18

134 www.aies-conference.com/.

Initiative on Ethics of Autonomous and Intelligent Systems,[135] the International Standards Organisation's JTC1/SC42 standardisation program,[136] and the 'Artificial Intelligence Ethics Framework' project at Australia's Data61[137] to issue standards or guidelines on the subject matter. Similarly, the 'Partnership on AI to Benefit People and Society' has formulated best practices for the use of algorithms in decision-making, including in relation to fairness, transparency and accountability.[138] Moreover, specific companies, such as Google, have done their own analysis on questions concerning "AI Governance" raising similar issues around explainability and fairness in automated decision-making.[139] Other regulatory options may include the use of third-party 'seals' attesting to particular qualities of algorithms. While not specifically focussed on government use of algorithms, it is possible that such voluntary standards will come to play a role in the regulation of automation for government decision-making in the (near) future.

7. Concluding Remarks

This Chapter sketched a preliminary taxonomy of government use of algorithms to automate decision-making in a variety of different areas, ranging from administrative law and judicial decision-making, to national security context and stature drafting. It discussed a plethora of problematic aspects and legal issues arising from the automation of government decision-making, including its potential incompatibility with the foundational legal values, such as the Rule of Law and specific issues arising in the context of national security and law enforcement. The tensions between increasing automation of government decision-making on the one hand, and the foundational values of public law on the other, are likely to escalate in the future. Therefore, it is paramount that the complex intersections between the two are urgently investigated, understood, and debated among the policy-makers, governments and the general public alike. It is crucial that these developments are also regulated so that individuals affected by government automation have venues for legal remedies, and more generally the future of government decision-making is compatible with foundational legal values and norms.

135 https://standards.ieee.org/industry-connections/ec/autonomous-systems.html

136 https://www.iso.org/committee/6794475.html

137 https://data61.csiro.au/en/Our-Work/AI-Framework

138 See their webpage at https://www.partnershiponai.org/.

139 Google, 'Perspectives on Issues in AI Governance', available at https://ai.google/perspectives-on-issues-in-AI-governance/.