Part 5: Objectivity and Criminal Law

§ 9 Algorithmic Crime Control between Risk, Objectivity, and Power

Lucia Sommerer[*]

* This contribution draws from and builds on the autor's PhD thesis, Lucia Sommerer, *Personenbezogenes Predictive Policing. Kriminalwissenschaftliche Untersuchung über die Automatisierung der Kriminalprognose* (Nomos 2020).

I. Introduction

Source: Petrarch, des Remèdes de l'une et l'autre fortune prospère et adverse, Paris, 1524.

Fortuna, the Roman goddess of destiny (left), and the goddess of wisdom and science Sapientia (right) are depicted in this 15th-century illustration in their traditional opposition. Fortuna's wheel lets people's fate rise and fall seemingly at random, her unpredictability posing risks, while science promises safety and objectivity. The attempt at a scientific 'taming of chance'[1] and thus the modern-day unification of the archrivals Fortuna and Sapientia lies at the core of the current expansion of algorithmic methods of predicting human behavior into more and more areas of crime control. This unification inadvertently brings about changes for the distribution of power and statistical likelihoods may be turned into 'legal truth'.[2] Behind the mathematical objectivity of algorithms may be looming a power shift in crime control, from traditional actors of crime control to computer scientists, from democratically legitimated modes of decision-making to processes lacking the involvement of the public, and from the logic of the law to the logic of the algorithm. A shift that is centred around the dominating category of our modern-day society: risk.[3]

This contribution will first take a look at the objectivity of algorithms (II.) and the power embedded in them (III.), before analysing a looming powershift in crime control affected particularly through reference to the seeming objectivity of mathematical models of chance (IV.).

---

1 Pictured already at Gerd Gigerenzer, *The Empire of Chance: How Probability Changed Science and Everyday Life* (Cambridge University Press 1997) xiii; Gerd Gigerenzer, *Risk savvy: How to make good decisions* (Penguin 2015) 44 ff ('By "taming chance" in Ian Hacking's evocative phrase (Hacking 1990), probability and statistics had reconciled Scientia to her archrival Fortuna.')

2 Jack Balkin, 'The Proliferation of Legal Truth' (2003) 26 Harv JL & Pub Pol'y 5, 6: '[L]aw creates truth – it makes things true as a matter of law. It makes things true in the eyes of the law. And when law makes things true in its own eyes, this has important consequences in the world.'

3 Ulrich Beck, *Risk society: Towards a new modernity* (Sage 1992).

II. Objectivity – Algorithms as a Neutral Tool?

'Do algorithms have politics?'
– in reference to Langdon Winner[4]
and
'If it's neutral, it's not technology.'
– Lance Strate[5]

Human decision-makers are not free of prejudice and subjective preferences,[6] quite the contrary. Harvard psychologists have shown with the so-called 'Implicit Association Test' that we may suffer from eg racist prejudices of which we are not even aware.[7] Studies on the criminal justice system have shown that judges tend to be more reluctant to grant an application for early release from prison before lunch than afterwards.[8] An algorithmic decision-making system is not subject to such individual preferences and fluctuations. For example, unlike a human brain, an algorithm can be strictly prescribed to ignore sensitive data such as skin color and religious affiliation as relevant input variables.[9] At first glance, algorithms thus have the potential to make decisions in a more neutral and less discriminatory way than humans.[10] But this appearance of neutrality

4 Langdon Winner, 'Do artifacts have politics?' (1980) 109 Daedalus 121, 122.

5 Lance Strate, 'If It's Neutral, It's Not Technology' (2012) 52 Educational Technology 6, 6; see already in the 1980s Winner (n 4), 122.

6 cf cognitive biases at Daniel Kahneman and Amos Tversky, 'Subjective probability: A judgment of representativeness' (1972) 3 Cognitive Psychology 430; see for Germany Gerd Gigerenzer, 'How to make cognitive illusions disappear: Beyond "heuristics and biases"' (1991) 2 Eur Rev Soc Psychol 83.

7 cf <http://implicit.harvatrd.edu> accessed 29 November 2021; cf also Mario Martini and David Nink, 'Wenn Maschinen entscheiden ... – vollautomatisierte Verwaltungsverfahren und der Persönlichkeitsschutz' (10/2017) 36 NVwZ-Extra 1; Linda Hamilton Krieger, 'The content of our categories: A cognitive bias approach to discrimination and equal employment opportunity' (1995) 47 Stan L Rev 1161 ff; Christine Jolls and Cass R. Sunstein, 'The Law of Implicit Bias' (2006) 94 Calif L Rev 969.

8 Shai Danziger, Jonathan Levav and Liora Avnaim-Pesso, 'Extraneous factors in judicial decisions' (2011) 108 PNAS 6889.

9 Timo Rademacher, 'Predictive Policing im deutschen Polizeirecht' (2017) 142 AöR 366 374 f.

10 cf Thomas Wischmeyer, 'Regulierung intelligenter Systeme' (2018) 143 AöR 1 26; Martini and Nink, 'Wenn Maschinen entscheiden ... – vollautomatisierte Verwaltungsverfahren und der Persönlichkeitsschutz' ; Anupam Chander, 'The Racist Algorithm?' (2017) 115 Mich L Rev 1023.

is deceptive. The widespread portrayal of algorithms as neutral, objective alternatives to human decision-making must be met with caution.[11] As *Kranzberg's* famous 'First Law of Technology' states[12] and as *Strate* in the above quotation implies, there is no such thing as truly neutral technology, and this is especially true of crime prediction algorithms. The use of algorithms does not fundamentally prevent discrimination; instead, human inequality is replaced by algorithmic inequality[13] and subjective, human preferences are hidden behind supposed neutrality and mathematical justifications.[14]

Like any other technology, algorithms, as man-made artifacts, are based on human decisions and thus, by definition, cannot work purely objectively and without the influence of these decisions. To put it bluntly, one can agree with *Strate* in the opening quote: If it is neutral, it is not technology.

For algorithms in crime control, too, programmers at all stages of the design process of the algorithm must make decisions that reflect their individual preferences and can perpetuate existing social inequalities. Given the large number of individual decisions in the algorithm design process, it is even possible that different developers who have been given the same task of designing an algorithmic crime predictions system may arrive at

---

11 cf Wischmeyer (n 10), 26; Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact' (2016) 104 Calif L Rev 671 673; see also Kelly Hannah-Moffat, 'The Uncertainties of Risk Assessment: Partiality, Transparency, and Just Decisions' (2014) 27 Fed Sent'g Rep 244 ff; Bernard E. Harcourt, 'Risk as a proxy for race: The dangers of risk assessment' (2014) 27 Fed Sent'g Rep 237, 240; Cecilia Klingele, 'The Promises and Perils of Evidence-Based Corrections' (2016) 91 Notre Dame L Rev 537, 538 ff; Sonja B. Starr, 'The New Profiling: Why Punishing Based on Poverty and Identity is Unconstitutional and Wrong' (2015) 27 Fed Sent'g Rep 229 ff.

12 'Technology is neither good or bad, nor is it neutral.' Melvin Kranzberg, 'Technology and History: "Kranzberg's Laws"' (1986) 27 Technology and Culture 544, 545.

13 Jessica M. Eaglin, 'Constructing Recidivism Risk' (2017) 67 Emory LJ 59, 97 f; cf Wischmeyer (n 10), 26; see also Kevin Macnish, 'Unblinking Eyes: the Ethics of Automating Surveillance' (2012) 14 Ethics and Information Technology 151 f; Engin Bozdag, 'Bias in Algorithmic Filtering and Personalization' (2013) 15 Ethics and Information Technology 209 ff; Barocas and Selbst (n 11), 672 ff; for police context see eg Kristian Lum and William Isaac, 'To predict and serve?' (2016) 13 Significance 14.

14 See Lucia Sommerer, *Personenbezogenes Predictive Policing. Kriminalwissenschaftliche Untersuchung über die Automatisierung der Kriminalprognose* (Nomos 2020) 105 ff.

very different algorithms that in practice produce two divergent risk scores for the same person.

1. *Sources of lack of objectivity*

Non-objectivity can enter an algorithmic system in many ways. In view of the complexity of the procedure, it is difficult to draw up a conclusive catalogue of all potential entry points of a programmer's value judgements and thereby biases and errors into the development of a seemingly neutral algorithm. Typical problems of data analysis in the area of crime control – which can only be sketched in broad strokes here – originate, however, in all phases of algorithm design: compiling the training data set, defining the target variables, defining the input variables, and calibrating and monitoring the machine learning process.

Decisive value judgements are, eg, how to deal with pre-existing biases in training data sets. Is the programmer recognizing pre-existing biases at all, is the programmer then counter-acting the biases? Or are pre-existing biases, eg against women's reintegration into the job market after pregnancy, even at all interpreted as biases in the training data or accepted as a statistical fact, that needs to be learned by the algorithm to be efficient. The latter is what the Austrian Employment Office argued for regarding an algorithm designed to distribute financial reintegration support into the labor market.[15] Deciding what is a bias in the training data that needs to be counteracted, and what is simply an accurate depiction of reality, is an important value judgement of a highly political nature. It will often depend on the individual programmers' attitudes whether or not unequal treatment is recognized as unjustified and therefore discriminatory or not.

Further value judgements are made when deciding how the programmer is translating the goal of knowing who will commit a crime in the future into a mathematical variable. Will they, out of comfort and convenience, select police custody or an indictment rather than a conviction as an indicator for a crime, as the target variable, even though not everyone who is taken into police custody, not everyone who is indicted is actually found guilty of a crime, and even though certain groups in society may be

15 Example at Wiebke Fröhlich and Indra Spiecker (gen. Döhmann), 'Können Algorithmen diskriminieren?' Verfassungsblog <https://verfassungsblog.de/koennen-algorithmen-diskriminieren/> accessed 29 November 2021.

at a higher risk of being taken into police custody unjustified without a subsequent conviction?

Further, through the decision for a certain input variable, the programmer often (unconsciously) decides that the algorithm will make more mistakes within a certain social group. Because how well certain input variables are suitable for predicting behaviour can differ for certain groups of society.[16]

Also, the programmer plays an important role in calibrating and overlooking the learning process of the algorithm. Core decisions are on the predictive accuracy and error rate of the algorithm, the ratio between false-negative and false-positive errors (asymmetric cost ratio) and the distribution of errors onto different subsets of society. The COMPAS-algorithm used in the US to support judges' sentencing decisions eg allegedly made false-positive errors (wrongly identifying an individual as 'high risk') twice as often for African Americans than for white Americans.[17]

Finally, the programmers at this point will have to make decisions that impact the probability of algorithm overfitting, ie, that the algorithms learn rules from a data set that are false, random correlation, not representative of actual connection between two variables in reality. Studies have also shown that data sets for minority groups often contain a higher degree of random correlations. There is therefore a risk that an algorithm may 'overfit' members of a minority group to a greater extent and thus make less accurate predictions – an issue that mindful programmers have to be aware of.

All these described value judgements can be used by programmers to discriminate against certain social groups and to hide their own discriminatory intentions behind the supposed objectivity of the numbers (so-called 'masked discrimination'). More often, however, programmers will unconsciously inscribe or perpetuate biases in an algorithm.

Since the inscription of biases in the design process can never be 100% avoided ex ante, it is all the more important to oblige manufacturers to

16 Barocas and Selbst (n 11), 688.

17 cf Julia Angwin and others, 'Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And it's Biased Against Blacks' ProPublica (23 May 2016) <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> accessed 29 November 2021; cf also differing error rates for face recognition technology, Sam Levin, 'Amazon Face Recognition Falsely Matches 28 Lawmakers With Mugshots, ACLU Says' The Guardian (26 July 2018) <https://www.theguardian.com/technology/2018/jul/26/amazon-facial-rekognition-congress-mugshots-aclu#img-1> accessed 29 November 2021.

actively search for biases in their systems and to have their algorithms reviewed by independent third parties.

Not only numerous scientists are critical of the advertising promises of neutral decisions by algorithms.[18] Skepticism of algorithmic neutrality seems to spread in the population in Germany, too. A population survey conducted by the Bertelsmann Stiftung in 2018 showed that only 6% of those surveyed agreed with the following statement: 'I think it's better if algorithms judge me instead of people. They make objective decisions that are the same for everyone.'[19]

2. *Is algorithmic lack of objectivity superior to human lack of objectivity?*

Once the assertion of neutral, non-discriminatory algorithms has been refuted, proponents of the use of algorithms often transition to arguing that unequal treatment by an algorithm is at least preferable to unequal treatment by humans; algorithmic discrimination is considered, so to speak, the lesser of two evils.[20] In favour of algorithms, it is argued that discrimination can be detected and eliminated more easily in algorithms than in humans.[21] However, this is a false conclusion: firstly, unequal treatment by an algorithm is extremely difficult for people to prove and secondly, algorithms threaten to act as a mathematical justification for existing discrimination instead of eliminating it.[22] An example of this is

---

18 cf Wischmeyer (n 10), 26; see Barocas and Selbst (n 11), 673; see also Hannah-Moffat (n 11), 244 ff; Harcourt (n 11), 240; Klingele (n 11), 538 ff; Starr (n 11), 229 ff.

19 Sarah Fischer and Thomas Petersen, *Was Deutschland über Algorithmen weiß und denkt. Ergebnisse einer repräsentativen Bevölkerungsumfrage im Auftrag der Bertelsmann Stiftung* (Bertelsmann Stiftung 2018) 25; cf however Center for the Governance of Change, *European Tech Insights 2019* (ie 2019) 10 ('25 % of Europeans are somewhat or totally in favour of letting an artificial intelligence make important decisions about the running of their country.').

20 cf already in the 1960s: 'Ultimately, there are no rational reasons for preferring manpower over machine power', Niklas Luhmann, *Recht und Automation in der öffentlichen Verwaltung* (Duncker & Humblot 1966) 60 fn 24.

21 I Bennett Capers, 'Race, Policing, and Technology' (2017) 95 NC L Rev 1241; cf also Timo Rademacher, 'Artificial Intelligence and Law Enforcement' in Thomas Wischmeyer and Timo Rademacher (eds), *Regulating Artificial Intelligence* (Springer 2020) mn 35.

22 cf Sonja B. Starr, 'Evidence-Based Sentencing and the Scientific Rationalization of Discrimination' (2014) 66 Stan L Rev 803 ('Scientific Rationalization of Discrimination').

the already mentioned justification strategy of the Austrian Employment Office for the use of an algorithm for the allocation of financial support for an individual's labor market reintegration, which generally wanted to give women and especially mothers less subsidies than men.[23] It was argued that the algorithm does not discriminate because it only reflects statistical realities in society, namely that women are statistically less likely to be successfully reintegrated into the labor market. With this argument, existing inequalities in society are consolidated rather than corrected by algorithms.[24]

As an argument against the preference of algorithmic discrimination over human discrimination, one should also keep in mind: once an algorithm contains a discriminatory preference, this can be much more far-reaching and affect more citizens than the subjective preference of one biased individual. Indeed, an algorithm is often designed to produce predictions *en masse*, which means that algorithmic discrimination is applied *en masse*. [25]

Still, others argue that algorithmic discrimination should be welcomed if it can only be shown that an algorithm discriminates *slightly less* than a group of human decision-makers it is designed to replace.[26] This argument must be rejected, however.[27] Quite apart from the fact that it will be difficult to provide reliable evidence that people actually discriminate to a greater extent than an algorithm, unconstitutional behaviour cannot be justified by reference to another form of unconstitutional behaviour. Just because discriminatory behaviour on the part of human government officers is unconstitutional, this does not mean that an algorithm that is only slightly less discriminatory is constitutional. The question of constitutionality has to be decided for each situation – human and algorithm – in isolation.

Algorithmic lack of objectivity is thus not *per se* superior to human lack of objectivity.

---

23 Example at Fröhlich and Spiecker (n 15).

24 See Sommerer (n 14), 105 ff.

25 cf Wischmeyer (n 10), 26.

26 cf Philipp Hacker, 'Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law' (2018) 55 Common Market L Rev 1143 1164 ('If this is the case [algorithmic decision making reduces bias vis-à-vis other types of (non-algorithmic) decision making], the use of the discriminating classifier should be considered appropriate as it maximizes the position of the marginalized group.').

27 Sommerer (n 14), 191 f.

III. Power – Algorithms as Man-Made Artefacts

'Nothing in itself is a risk, there is no risk in reality.
Conversely, everything can be a risk, everything
depends on the way one analyses the danger,
looks at the event.'
– François Ewald, L'état providence [The Welfare State][28]

This section will first examine how the output of algorithms as seemingly objective truths stifles controversy (1.), and secondly, look at the man-made nature of the category at the core of all crime technology, ie risk (2.).

1. Concealing controversy

It has already been noted for the rise of statistics in crime control at the end of the 20th century that the application of supposedly objective mathematical models to complex societal issues inconspicuously conceals controversy and suppresses public discourse on these issues.[29] This phenomenon is exasperated by the use of ever more opaque[30] algorithms in present times. The concealment of man-made policy decisions and value judgements through a discursive framing as supposedly objective and without alternatives is inherent in algorithmic crime predictions.[31] In this concealment lies power. Statistical procedures divide people into different 'classes', which would actually be perceived as offensive in society and in the legal system if it were not for these mathematical, algorithmic methods: Algorithmic methods have the 'ideological power' to defuse or completely hide the moral value judgement that lies in the classification of humans.[32] 'Algorithmic Justice' thus leads to a superficial 'scientification' of criminal policy,[33] which is, however, indeed not one. In fact, the idea of a strictly rational, mathematical determination of crime risks is not

28 François Ewald, *Der Vorsorgestaat: aus dem Französischen von Wolfram Bayer und Hermann Kocyba: mit einem Essay von Ulrich Beck* (2 edn, Suhrkamp 1993) 210.
29 Jonathan Simon, 'The Ideological Effects of Actuarial Practices' (1988) 22 Law & Soc'y Rev 771 792.
30 See Sommerer (n 14), 165 ff.
31 ibid, 300 ff.
32 Simon (n 29), 794.
33 cf Starr (n 22) ('Scientific Rationalization of Discrimination').

very realistic.[34] It neglects the fact that the definition of risks is ultimately guided by non-objective interests. It avoids the question of which risks the focus is to be put on and ignores the fact that the decision as to when a risk is no longer tolerable is a value decision.

2. *Risk as a non-objective category*

The power embedded in the concealment and suppression of controversy via algorithms can be illustrated further by taking a closer look at the non-objective nature of the term 'risks', the central category of crime control in the 21st century.

a. *Man-made definitions of risk*

A risk always carries within itself an inherent reference to the future and a certain call to action[35]: it describes the possibility of a future evil, which at the same time normatively establishes a duty to act, a behavioural imperative in the present.[36] As the French philosopher and sociologist *Ewald* notes in the opening quotation, almost anything can be declared a risk.[37] Ultimately, the justification for naming something as a risk is a narrative, a coherent story that explains why one has to protect oneself in a concrete situation and in what specific way.[38] Successful risk narratives are often used to justify political action, especially in the crime control arena, but

34 cf Karl-Ludwig Kunz, 'Grundzüge der heutigen Kriminalpolitik' (2005) 17 NK 151, 154.

35 Franz-Xaver Kaufmann, *Sicherheit als soziologisches und sozialpolitisches Problem. Untersuchungen zu einer Wertidee hochdifferenzierter Gesellschaften*, vol 4 (LIT Verlag 2012) 258.

36 ibid.

37 ibid; Bernd Dollinger, 'Sicherheit als politische Narration: Risiko-Kommunikation und die Herstellung von Un-/Sicherheit' in Bernd Dollinger and Henning Schmidt-Semisch (eds), *Sicherer Alltag? Politiken und Mechanismen der Sicherheitskonstruktion im Alltag* (Springer 2016) 57 f.

38 ibid, 58; on coherent stories for location based predictive policing Simon Egbert, 'On Security Discourses and Techno-Fixes – The Political Framing and Implementation of Predictive Policing in Germany' (2018) 3 European Journal for Security Studies 95.

also in many other areas such as health or the environment. [39] Risk cannot be thought of independently of security and normality. *Dollinger* rightly states: There must be stories and ideas of a 'risk-free or safe life in order to be able to delimit and scandalize risks as special phenomena'.[40] This means that the characteristic of being risky is not unchangeably inscribed in a situation or person. Risk is not a descriptive term,[41] as it is possible to objectively determine and describe that a person is blond or has brown eyes. According to this view, situations only become a risk when they are assigned this very social meaning.[42] Only in this process of assigning meaning can risks be *experienced as* reality, as *Ewald* also states in the opening quotation when he notices that there is no risk *in* reality.[43] Whoever defines risks (through human or algorithmic calculations) thus actively produces a new reality with a claim to truth instead of merely describing an existing one. This is the performative effect of the concept of risk.[44] 'The productions of truth', *Foucault* emphasizes, 'cannot be separated from power and power mechanisms, because on the one hand power mechanisms enable and induce the production of truths, and on the other hand the production of truth also has power effects with a binding force on us.[45] Those who define risks thus exercise power over social reality.[46]

---

39 cf Deborah A Stone, 'Causal Stories and the Formation of Policy Agendas' (1989) 104 Political Science Quarterly 281; see also Michael D Jones, Mark K McBeth and Elizabeth A Shanahan, 'Introducing the Narrative Policy Framework' in Michael D Jones, Mark K McBeth and Elizabeth A Shanahan (eds), *The Science of Stories* (Springer 2014).

40 Dollinger (n 37), 57 f.

41 ibid.

42 ibid, 57.

43 ibid.

44 cf also Tobias Singelnstein and Peer Stolle, *Die Sicherheitsgesellschaft: Soziale Kontrolle im 21. Jahrhundert* (3rd edn, Springer-Verlag 2012) 199 (‚By making risk and danger prognoses, they [the police] gain the power to define social reality'); cf also Hartmut Wächtler, 'Strafverteidigung und soziale Bewegungen. Die 1980er Jahre' in Strafverteidigervereinigungen (ed), *Kein Grund zu feiern: 30 Jahre Strafverteidigertag* (Organisationsbüro der Strafverteidigervereinigungen 2007) 136.

45 Michel Foucault, 'Macht und Wissen' in Michel Foucault (ed), *Dits et Ecrits Schriften* (Surkamp 2003) 521.

46 cf also Niklas Creemers and Daniel Guagnin, 'Datenbanken in der Polizeipraxis: Zur computergestützten Konstruktion von Verdacht' (2014) 46 KrimJ 134 137; Christian Fuchs, *Krise und Kritik in der Informationsgesellschaft* (Libri 2002) 22; cf also *Dubarle*, who called the methods of ruling of Hobbes' Leviathan 'harmless fun' compared to the possibilities of the computer, cited at Thomas Wischmeyer, '§ 21 Regierungs- und Verwaltungshandeln durch KI' in Martin Ebers and others

b. Uneven distribution of risks

Further it must be noted that risks can be unequally distributed in society and, as already recognized by *Beck*, sometimes adhere to a class scheme, just like the distribution of wealth.[47] Thus majority decisions on accepting risks can oblige certain minority groups in society to take on excessive risks.[48] Sometimes a decision may even only superficially be about minimizing risks, when in fact it is the distribution of risk that is being decided.[49] An unequal distribution also applies to risks in crime control.[50] Thus, certain groups in society may be more vulnerable to becoming the victim of a particular crime. For example, members of lower social classes are more likely to be victims of violent crime.[51] But the use of certain crime control technologies may also put certain minority groups at greater risk of being falsely identified as risky. This is demonstrated eg by the COMPAS-algorithm for sentencing decisions[52] or by face recognition technology designed to identify wanted criminals[53] which have been reported to make significantly more mistakes for African-Americans than for white Americans.

c. Tolerated risks

There is no absolute certainty. The German Federal Constitutional Court also expressly states (in connection with a lawsuit against the construction of a nuclear power plant) that society as a whole must tolerate certain residual risks.[54] In road traffic, we tolerate high risks and have decided to make these risks manageable with an insurance approach, ie motor vehicle

(eds), *Rechtshandbuch Künstliche Intelligenz und Robotik* (CH Beck im Erscheinen [vrsl. 2020]) 41.

47 Ulrich Beck, *Risikogesellschaft: Auf dem Weg in eine andere Moderne* (Suhrkamp Verlag 1986) 46; particularly risky risk industries are outsourced to poor countries on the periphery, ibid 56

48 Gerhard Banse, *Risiko – Technik – Technisches Handeln (eine Bestandsaufnahme)* (Kernforschungszentrum Karlsruhe 1993) 9.

49 ibid, 20.

50 Karl-Ludwig Kunz and Tobias Singelnstein, Kriminologie: eine Grundlegung (7th edn, UTB 2016) § 18 mn 22 ff.

51 ibid, § 18 mn 22.

52 cf Angwin and others (n 17).

53 cf Levin (n 17).

54 BVerfGE 49, 89, 137 f.

liability insurance, instead of avoiding them altogether by banning cars. Victims of road traffic are to be understood as a system-immanent sacrifice of a society interested in mobility. Similarly, one can say that victims of crime are generally to be understood as a system-immanent price of a society interested in liberal, democratic and constitutional values, without total surveillance of its citizens. At what point a risk is no longer tolerated – which, conversely, can also be formulated as the question: how safe is safe enough? – cannot be answered by a mere stochastic, algorithmic calculation, but only by an evaluative discretionary decision on justifiability.[55] The goals and values that are the basis of this decision are not unchangeably fixed, but depend on the situation and time. The definition of the threshold for a tolerated risk often proves to be not exactly justifiable.[56]

Kunz emphasizes that a risk, unlike a danger, only arises in the *perception* as such. He thus also emphasizes the social construction of risk.[57] In doing so, the performative effect of the risk prediction itself must be emphasized: only through the possibility of prediction does a risk come into focus. 'With the increase in knowledge about causal chains of effects, society has instruments and institutions at its disposal to predict negative events and their consequences (anticipation) and to design or implement appropriate countermeasures. At the same time, this increases the moral requirement to take risk precautions in order to exclude or limit negative events'.[58] The less a risk can be predicted, the less power to act in this respect is narratively placed in the sphere of human control, the higher the risk tolerance is in practice.

The key points of the concept of risk, the basis of all seemingly objective algorithmic crime prediction technology, can be summed up as the following:

– A situation only becomes a risk through social attribution based on a narrative.

---

55 cf in criminal law dogmatics the 'permissible risk' (*erlaubtes Risiko*); see also in different context Georg Freund, *Normative Probleme der "Tatsachenfeststellung": eine Untersuchung zum tolerierten Risiko einer Fehlverurteilung im Bereich subjektiver Deliktsmerkmale* (Müller, Jurist Verlag 1987) 198.

56 Banse (n 48), 21

57 Karl-Ludwig Kunz, *Kriminologie: eine Grundlegung* (6th edn, UTB 2011) 339; Kunz and Singelnstein (n 50), 340 ff.

58 Ortwin Renn, 'Risikowahrnehmung und Risikobewertung: soziale Perzeption und gesellschaftliche Konflikte' in Sabyasachi Chakraborty and George Yadigaroglu (eds), *Ganzheitliche Risikobetrachtungen Technische, ethische und soziale Aspekte* (Springer 1991) 6 ff.

– The identification of risk has an inherent performative effect.
– There are tolerated risks. The point at which a risk can no longer be tolerated represents a value judgement.

We can thus state at this point that algorithms are based on and contain many political value judgements that are oftentimes concealed, invisible to the outside world wherein – to speak with *Foucault* – a power for the definition of realities lies. We can also confirm the connection between objectivity and power, ie that power is in fact embedded and at the same time concealed in the use of algorithms, particularly because of its presentation as objective.

IV. Powershift

After confirming the connection between objectivity and power, this contribution will now focus on the specific power*shifts* accompanying an increasing use of algorithms in a crime control. First a powershift away from the public eye will be discussed (1.). Further, powershifts occur away from traditional actors in crime control, away from law enforcement officials (2.) and away from courts (3.), culminating in a shift of algorithms from mere tool to authority figure in crime control (4.) and from the logic of the law to the logic of the algorithm (5.).

1. Away from the public eye – undemocratic decision-making

Many of the decisions mentioned above should rather be made in a democratically legitimized manner. Algorithmic crime predictions as man-made artefacts are necessarily based on political premises, which are, however, not revealed and discussed as such. The political discussions that have taken place so far (at best) extend to the question of *whether* an algorithmic system that is *already* represented as neutral and objective should be applied or not. The current public discussions do not touch on the important political questions of the many just mentioned value decisions made when developing an algorithmic prediction system.

Whether it should be a valid approach at all to apply statistical knowledge about groups of people to an individual and on this basis restrict constitutional rights, ie whether we want to reproach an individual for sharing characteristics with a group of people, of which a large proportion have committed crimes in the past, are complex questions and require thorough

democratic debate.[59] Other already mentioned value decisions that are hardly ever identified as such are the questions of what false-positive rate is still acceptable to society (ie the number of persons falsely identified as highly dangerous in order to detect one *actually* highly dangerous person), and the question of the degree of probability beyond which a person may be labelled 'highly dangerous'. Finally, another highly political issue is the response to statistical discrimination, ie the different treatment of persons by a predictive algorithm, resulting from possibly pre-existing inequalities in the training data.[60]

All of these are highly political decisions that are likely to be taken differently by politicians across the political spectrum. Ultimately the fundamental issue here is one of distribution of state resources in the fight against crime, and a matter of determining how we as a society want to live. Yet there is a danger that public debate on these matters will be suppressed by simple reference to the supposedly objective calculations done by an algorithm. An 'algorithmization' of crime control thus threatens to be detrimental to public debates on issues of crime control. By removing certain issues from public debate power, too, is shifted away from the public. The power to question, discuss and decide on these issues then does not longer lie with the public but with whomever was able to embed their now unquestioned value judgement in the algorithm design in its developmental phase.

2. *Away from law enforcement officials – de-skilling*

Powershifts also occur from traditional actors in crime control onto the computer sciences. Legal practitioners might lose their ability to judge.[61] The use of an algorithm may be 'de-skilling' them, putting them in a situation where they on the one hand after a while cannot do without the

---

59 It is a constitutional requirement that in the fundamentally normative sphere, especially in the area of the exercise of constitutional rights, the parliamentary legislator must regulate all essential prerequisites of state intervention itself (*Wesentlichkeitsgebot*); see particularly for person-based predictive policing Sommerer (n 4), 137 f.; in general Victor Jouannaud, 'The Essential-Matters Doctrine (*Wesentlichkeitsdoktrin*) in Private Law: A Constitutional Limit to Judicial Development of the Law?' (§ 7).

60 In detail on the issue of discrimination Sommerer (n 14), 105 ff, 171 ff.

61 Nadja Capus, 'Die Tyrannei des Wahrscheinlichen in der Justiz' Die Republik (19 September 2018) <https://www.republik.ch/2018/09/19/die-tyrannei-des-wahrscheinlichen-in-der-justiz> accessed 29 November 2021.

algorithm anymore, and on the other hand cannot understand or review the algorithms decision themselves anymore. Such loss of human expertise and the growing dependency on machine rationality is already apparent in other areas of automation (eg aviation, medicine).[62] If de-skilling occurs the human is *de facto* only executing a higher authorities orders without being able to replace or question them. If de-skilling occurs in crime control this shifts power away for the publicly accountable individual civil servant that has to decide each situation in front of them, and places it on the humans that have in the past (shielded from the public eye) shaped the different stages of algorithm design and thereby shaped the algorithms output now followed by the civil servant. This shifts power onto the computer and data scientist developers of the algorithms.

3. Away from the courts – limited legal scrutiny due to complexity

A further shift away from the power of the law may occur if the competent legal authorities such as courts effectively limit their level of scrutiny of decisions that were made based on algorithmic output, due to its general claim to objectivity together with complexity and opacity of the methods involved.

Such limited scrutiny may occur eg for discriminations by an algorithm. An algorithm will generally *automatically* be able to give an initial statistical justification for any unequal treatment of two groups done by it. A refutation of this initial statistical justification may not be easy and take great effort, eg experts looking into the algorithms training data and calibration process.

It is therefore to be feared that for the review of algorithmic predictions there will be a *de facto* reversal of the burden to bring arguments and proof. In principle, in anti-discrimination law the burden of proof rests with the entity that is treating someone unequally as soon as the person concerned presents a case of unequal treatment.[63] In the case of algorithmic discrimination, however, the person affected by the unequal treatment seems to bear a doubled burden of proof: first, for proving the existence of

62 See for 'de-skilling' in detail Nicholas Carr, *The Glass Cage: Automation and Us* (WW Norton & Company 2014).

63 cf Alexander Tischbirek, 'AI and Discrimination: Discriminating against Discriminatory Systems' in Thomas Wischmeyer and Timo Rademacher (eds), *Regulating Artificial Intelligence* (Springer 2020) mn 20.

unequal treatment and second, for the refutation of the statistical justification automatically generated by the algorithm.[64]

At the same time, it is to be feared that the judicial review of such automatedly generated statistical justifications will be rather generous, ie that courts will limit their standard of review to a control for arbitrariness (*Willkürkontrolle*), simply due to the technical difficulty and complexity of an in-depth review of algorithms' inner workings. As a consequence, the state using an algorithm will be granted a wide scope of decision-making in the selection and evaluation of correlations, even in areas highly sensitive to fundamental rights.

Such a development must be counteracted, since the German Federal Constitutional Court (BVerfG) has in recent years quite deliberately moved away from the standard of mere arbitrary control, according to which in the past any reasonable argument that did not appear completely arbitrary was sufficient to justify unequal treatment.[65] In the case of distinctions on the basis of personal characteristics, and in a context that also encroaches on other civil liberties (both the case for algorithmic crime predictions) the Federal Constitutional Court today states that courts must apply a much stricter standard of justification (a *de facto* proportionality test).[66] For algorithms such different standards of review makes the difference between asking: 'Are there *obvious* signs that make the algorithm appear arbitrary or non-objective?', or: 'Is a treatment justified based on an *in depth, over all* evaluation of the algorithms' mathematical models, input and training data?'

If courts resign themselves to only ask the first question, the power of a particularly strict review of the courts *vis a vis* government actions regresses. Courts then effectively give up part of their power bestowed onto them by the Constitutional Court when faced with algorithms that are just too complex and time consuming to understand and review in detail.

64 Fröhlich and Spiecker (n 15).

65 Angelika Nußberger, 'Art 3' in Michael Sachs, *Grundgesetz. Kommentar* (CH Beck 2018) mn. 33; Volker Epping, *Grundrechte* (8th edn, Springer 2019) 795.

66 BVerfGE 129, 49, 68 f; see overview for the criteria to determine the intensity of review at Nußberger (n 65), mn 90 ff.

4. From tool to authority figure – algorithmic thoughtlessness

With the term 'thoughtlessness' *Hannah Arendt* described how ordinary people in the Third Reich could commit war crimes by switching off their independent thinking without having decidedly 'evil' intentions. An essential factor in the emergence of such an attitude was the integration into a bureaucratic apparatus. The Nazi war criminal *Eichmann*, for example, repeatedly referred to having merely followed instructions. *Arendt* saw the great danger here in the inability of people to reflect on the scope of their own actions. This inability could, under certain circumstances, affect almost every average person, in which Arendt saw the 'banality' of evil.

Of course, predictive algorithms do not linearly lead to crimes against humanity. And yet the concept of 'thoughtlessness' is also useful in an algorithmic context since it expresses how people in a system rely on the decisions of others, do not question them, simply follow them. As justification, they refer to the higher authority and the need to follow rules in the interest of the functioning of the system. This situation is quite comparable to the way people deal with the result of algorithmic calculations.

Even though algorithm-based systems were initially conceived only as a tool subordinated to the user, in practice they are likely to take on a more dominating role. Algorithms can take on a role similar to that of an authority figure to which the user looks up, such as a superior whose 'orders' are executed without question. Psychological studies of decision support systems in medicine and aviation have shown that people find it very difficult to make a decision that would contradict the result of algorithmic calculations.[67] This phenomenon, known as 'automation bias' leads people to refrain from obtaining and evaluating information themselves, even to deliberately ignore evidence that is clearly in conflict with the result produced by an algorithm. People are less confident in their own expertise than in the complex, opaque algorithmic processes. This is all the more true if in light of time pressure and rationalization making decisions *against* 'the machine' involves a greater expenditure of time and

67 See Dietrich Manzey, 'Systemgestaltung und Automatisierung' in Petra Badke-Schaub, Gesine Hofinger and Kristina Lauche (eds), *Human Factors –Psychologie sicheren Handelns in Risikobranchen* (2nd edn, Springer 2012) 333; Linda J Skitka, Kathleen L Mosier and Mark Burdick, 'Does Automation Bias Decision-Making?' (1999) 51 Int J Hum Comput Stud 991; Kathleen L Mosier and others, 'Automation Bias: Decision Making and Performance in High-Tech Cockpits' (1998) 8 Int J Aviat Psychol 47 63.

explanatory effort than making decisions *in line with* 'the machine'. As a result, algorithmic calculations which were only intended as support for human decision-making (ie a mere tools), in fact completely determine the human decision. The human operator outsources responsibility to the algorithmic processes. In this constellation, the algorithm's supposedly reliable predictions ultimately become the decisive authority figure. The human succumbs to 'thoughtlessness', in light of the imposition of having to make a decision. Uncertainty demands normative decisions from humans, a demand we are tempted to free ourselves from by following the certainty that the algorithm seems to offer. The more a process is automated, the easier it is for people to become 'thoughtless' and indifferent to its results. The more crime control is automated, the easier it is for government officials using the system to feel no longer responsible for actions taken on the basis of the system. Ultimately, this, too, is a question of shifting responsibility from the traditional actors of crime control to computer scientists.[68]

5. From the logic of the law to the logic of algorithms – 'machine logic'

'If one applies [statistical] laws (...)
to the objects of politics and history indiscriminately,
then these objects have already been willfully, quietly obliterated,
namely they have been levelled as deviations
into the medium in which they appear, but which they are not.'
– Hannah Arendt, Vita Activa[69]

The logic of the law and the logic of the algorithm are at odds.[70] The question is whose mode of 'thinking' will prevail during the present algorithmic turn in crime control. 'Machines' make decisions in different ways, fact-finding and prognoses are made on a different basis than humans.

---

68 Sommerer (n 14), 327 ff.

69 Hannah Arendt, *Vita Activa or Vom tätigen Leben* (Pieper 1994 [1958]) 43. [*German original*: 'Wendet man also die [statistischen] Gesetze (...) unbesehen auf die Gegenstände der Politik und der Geschichte an, so hat man diese Gegenstände bereits unter der Hand eliminiert, sie nämlich als Abweichungen in dasjenige Medium eingeebnet, in dem sie zwar erscheinen, das sie aber gerade nicht sind.'; translation by author.]

70 cf also Eric Hilgendorf, '"Die Schuld ist immer zweifellos?" – Offene Fragen bei Tatsachenfeststellung und Beweis mit Hilfe "intelligenter" Maschinen' in Thomas Fischer (ed), *Beweis* (Nomos 2019) 249 (discussing a departure from the logic of the law through the use of AI in criminal justice contexts).

Hilgendorf calls this a 'paradigm shift' and 'no less than another way of establishing the truth.'[71]

Will law subordinate technology, harness its powers in its own interests, mould it to its own internal logic, as concepts such as 'privacy by design' or 'transparency by design'[72] may imply? Are the new algorithmic models of knowledge creation and processing to be considered a gift for the legal system that will enable it to even expand its reach and strengthen the rule of law?

In short, will we be able to embed the values of the law into technology, or will technology embed its values into the law? Will technology subjugate the law to its own internal logic? Will the new technological possibilities change our perception and interpretation of even the most fundamental legal guarantees and institutions?

The latter is not as far-fetched as it may seem. The basic prerequisites that have led to the current form and function of our legal system are changing. Even firmly established pillars of the legal system such as the principle of the rule of law can prove less stable than expected in the face of technological change.[73] Our legal system has always been decisively shaped by technologies and it cannot be thought of independently of them. Our current legal system is particularly shaped by three technologies of knowledge production and retention: language, writing and printing.[74]

---

71 ibid, 250.

72 Karen Yeung, '"Hypernudge": Big Data as a mode of regulation by design' (2017) 20 Information, Communication & Society 118; Mireille Hildebrandt, 'Legal Protection by Design. Objections and Refutations.' (2011) 5 xx Legisprudence 223; Paolo Balboni and Milda Macenaite, 'Privacy by design and anonymisation techniques in action: Case study of Ma3tch technology' (2013) 29 Computer Law & Security Review 330.

73 Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (Edward Elgar 2015) 47 ff; Mireille Hildebrandt, 'Law as Information in the Era of Data-Driven Agency' (2016) 79 Mod L Rev 1 3. Her approach is an extension of earlier theories of media analysis by eg Marshall McLuhan to the field of law. See her reference to him in Hildebrandt, *Smart Technologies* (n 73), 49; McLuhan assumes that changes in the dominant forms of communication (ie the carriers of knowledge production) lead to fundamental changes in human thinking; see Marshall McLuhan, *The Gutenberg Galaxy: The Making of Typographic Man* (Toronto University Press 1962); Marshall McLuhan, *Understanding Media: The Extensions of Man* (MIT press 1994 [1964]); see also Walter J Ong, *Orality and literacy* (Routledge 2012 [1982]).

74 Hildebrandt, 'Law as Information' (n 73), 3; cf also Pierre Legendre, *De la société comme texte: linéaments d'une anthropologie dogmatique* (Fayard 2001) 17 ('Man can only access the world through the mediation of the medium of language and thus through representation').

If the significance of the processing of information through language and writing is reduced and replaced by new technologies of knowledge production, which differ substantially from its predecessors, this can have an effect on the basic structures of the legal system. The production and storage of knowledge in algorithmic form, which is no longer *directly* accessible to humans, can be regarded as a technological revolution with culture-changing significance in this regard. [75]

The view of the fundamental pillars of our legal system as monolithic and immutable is thus highly doubtful,[76] and cannot be blindly relied on. Some authors fear the legal system's fundamental pillars could be in danger if algorithms transfer their own rationalities and understandings of the world into the law and into crime control. The algorithmic rationalities, the 'machine logic' so to speak, would then become the basis for governmental and regulatory decisions, leading to a fundamental shift in values and, in the long run, even to a possible self-destruction of the legal system.[77] According to the story of Ulysses in Homeric poetry, the Trojans joyfully moved a wooden horse they thought was a gift left at their gates into their secure city. There, however, Greek warriors disembarked

75 Victor Mayer-Schönberger and Kenneth Cukier, *Big Data – A Revolution that will transform how we live, work and think* (Houghton Mifflin Harcourt 2013) 30.

76 Hildebrandt, 'Law as Information' (n 73) 2 ('We cannot take for granted that law will interact with an artificially intelligent information and communications technology infrastructure (ICTI) in the same way as it has interacted with written and printed text.'; 'We cannot take for granted that the current mode of existence of law and the Rule of Law are sustainable once the ICTI of data-driven agency takes over.').

77 cf Ian Kerr, 'Digital prophecies and web intelligence' in Mireille Hildebrandt and Katja de Vries (eds), *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology* (Routledge 2013) 105 ('a broad uptake of predictive and preemptive approaches across the social order might reach a tipping point wherein our systems of social control could no longer properly be called a "legal system".'); cf opposition of 'government by the law' and 'algorithmic government' by Antoinette Rouvroy, 'Political and Ethical Perspectives on Data Obfuscation' in ibid, 143; more cautious Monika Zalnieriute, Lyria Bennett Moses and George Williams, 'The Rule of Law and Automation of Government Decision-Making' (2019) 82 Mod L Rev 425 455 ('The rule of law is not a static concept. It evolves in response to changing societal values and the operation of government. As technology reshapes society, and government interacts with the community, it can be expected in turn that our understanding of the rule of law will shift. Values such as transparency and accountability, predictability and consistency and equality before the law may remain central to conceptions of the rule of law, but their interpretation and application may change.').

from the horse and destroyed Troy from the inside.[78] The object, which at first seemed like a gift, turned out to be disastrous in retrospect. By adapting it to established cultural techniques (the exchange of gifts) and its symbolism (the peaceful withdrawal of the Greeks), which was welcome in the situation, the Greeks induced the Trojans to participate in their own destruction. Pointedly, some modern-day authors[79] could be given the name of *Laocoon*,[80] because they fear that now, as new technologies such as algorithmic crime predictions stand at the gates of jurisprudence, they too could turn out to be an unwholesome gift and take over the law from within. In the discourse, popular authors,[81] but also legal scholars[82] and philosophers[83] critically noted that algorithms-based decision systems transform an area from the inside once they have established themselves in it. This transformation consists in a subordination to the 'logic and rationalities of the machine', or, as *Arendt* formulated it for statistical procedures, in the 'levelling' of algorithm-external areas of life *into* machine logic and thereby extinguishing the areas' pre-existing idiosyncrasies and modes of thinking.

The term 'machine logic' in this context refers to a totality of interwoven mutually reinforcing phenomena accompanying the current algorithmic turn:

- The focus on correlations instead of causalities and an impending resignation to decision-making systems that – like eg neural networks – operate beyond the human comprehensible. [84]
- The limitation of the legal system's field of vision to the mathematically quantifiable.

78 See Hom Od 4, 271–289; 8, 492–520; 11, 523–532.

79 cf Kerr (n 77), 105; generally critical of algorithmic processes Cathy O'Neil, *Weapons of Math Destruction – How Big Data Inceases Inequalities and Threatens Democracy* (Crown Publishers 2016); for use in crime control *ibid*, 26 ff, 71 ff; cf for the importance of different technologies as a prerequisite for the (further) development of a legal system Hildebrandt, *Smart Technologies* (n 73), 47 ff.

80 Laocoon warns the Trojans of the horse using his spear to stab the horse in order to examine it for threats from within, Verg Aen II, 40–53.

81 cf O'Neil (n 79).

82 cf Zalnieriute, Moses and Williams (n 77), 455; Kerr (n 77), 105.

83 cf Hildebrandt, *Smart Technologies* (n 73), 47 ff; Rouvroy (n 77), 143.

84 See Joshua A Kroll and others, 'Accountable Algorithms' (2017) 165 U Pa L Rev 633 638; Will Knight, 'The Dark Secret at the Heart of AI' MIT Technol Rev <https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/> accessed 29 November 2021.

- A view of 'social physics' – represented eg by *Pentland* [85] – and 'data behaviorism' – as described by *Rouvroy* [86] – according to which all human behaviour can be calculated as if it were a scientific phenomenon; a view in conflict with the presumption of free will, underlying the legal system.[87]
- The reduction of human beings to data processes, [88] in the words of the computer theorist *Negroponte*, to 'information bits'[89], and the neglect, if not the negation of their characteristics as sentient, thinking beings.
- The lack of disclosure of the normativity of algorithm-based decisions in the legal system.
- The impending inability of humans to make practical decisions against the predictions of a complex algorithmic system (automation bias).
- The loss of human expertise and the growing dependence on machine rationality that is already apparent in other areas of automation (deskilling).
- The adoption of efficiency as a leitmotif in the entire control of crime and a subsequent relaxation of legal guarantees such as the principle of equal treatment in Article 3 of the German Constitution.

Each of these phenomena brings its own challenges, and the list of challenges could be extended further. However, it is precisely the interplay of all these phenomena, so the concern is in legal scholarship, that the law as the leading variable of crime control could be displaced or fundamentally changed from within.

So far, there is little empirical evidence that such a change is actually taking place. The technology is still in its infancy in Germany. Due to the multitude of possible applications and different technical designs of predictive algorithms, no general statement can be made about the overall impact of algorithmic crime control. The question of whether it will actually turn out to be an ominous gift for the legal system cannot yet be

85 Alex Pentland, *Social Physics: How Good Ideas Spread – the Lessons from a New Science* (WW Norton & Company 2014).

86 Rouvroy (n 77) 143 ff.

87 See Wolfgang Prinz, 'Der Wille als Artefakt' in Karl-Siegbert Rehberg (ed), *Die Natur der Gesellschaft* (Campus Verl 2008) 593; Eduard Dreher, *Die Willensfreiheit: ein zentrales Problem mit vielen Seiten* (Beck 1987) ff; cf also BGHSt 2, 194, 200 ('The inner reason for the accusation of guilt lies in the fact that man is designed for free, responsible, moral self-determination […]').

88 cf also Jens Puschke, *Legitimation, Grenzen und Dogmatik von Vorbereitungstatbeständen*, vol 12 (Mohr Siebeck 2017) 256.

89 Nicholas Negroponte, *Being Digital* (Hodden&Stoughton 1995).

answered with certainty. Nevertheless, the existing concerns must not be ignored. Rather vigilance and an active questioning of algorithms by legal scholars is required to ensure that the described concerns do not become reality.

V. Conclusion

It can be concluded: The exercise of power in crime control with the help of statistics quietly and inconspicuously suppresses controversy particularly through reference to algorithms' supposed objectivity. The use of algorithms presented as mathematically objective, fair and neutral leads to the concealment of underlying man-made policy decisions and value judgements.[90] The seeming objectivity of the algorithms facilitates a powershift away from the public, away from the rationalities of the law. To ensure that the power struggle between the logic of the law and the logic of algorithms is decided in favour of the former two steps are required: firstly, legal scholars and practitioners must be made more knowledgeable about statistical, computer science methods (to know where and when to question them).[91] Secondly, novel control architectures for crime prediction algorithms must be installed. The review of compliance of algorithms with the law must not be left to individual legal proceedings which could overwhelm courts, but must be carried out systematically and preventively,[92] ie before the law is infringed, by an independent governmental standard setting and review body. Such control architecture for crime predictions is yet inexistent as of today. If these steps are not taken, algorithms threaten to perpetuate and reinforce existing prejudices and hidden value judgements behind a façade of mathematical clarity and neutrality.[93] If algorithms set rules like law, if programmers and data scientist turn into *de facto* lawmakers, the architecture of algorithms will have to be interrogated just as we interrogate the codes created by parliaments.[94]

---

90 Sommerer (n 14), 300 ff.

91 cf Tischbirek (n 63), mn 44 f ('paradigm of knowledge creation').

92 cf ibid, mn 45.

93 Creemers and Guagnin (n 46) 136.

94 Lawrence Lessig, 'Code Is Law: On Liberty in Cyberspace' Harvard Magazine (1 January 2000) <http://harvardmagazine.com/2000/01/code-is-law-html> accessed 29 November 2021; Lawrence Lessig, *Code: And Other Laws of Cyberspace* (2nd edn, Basic Books 2006) 1 ff.