Uncertainty, Risk and Responsibility

The Security of the Future – Artificial Intelligence and Social Control.
From Predictive Policing to Social Scoring

Tobias Singelnstein

Artificial intelligence[1] *will have an impact similar to the invention of electricity. With this much-quoted statement, computer scientist and Stanford professor Andrew Ng has summarised the formative role of artificial intelligence (AI).*[2] *Just like electricity in the 19th and 20th centuries, AI is a technology that will find its way into practically every area of life and change them more or less fundamentally. The world of crime and criminal sciences is no exception. The new technologies and the understanding on which they are based will lead to a completely different societal understanding of security and its threats in the coming decades. For not only does deviant behaviour shape the measures that society takes – from a constructivist perspective, it is rather that, contrary to this common understanding, the way in which deviance is dealt with determines how it is seen, understood and conceptualised.*

A. Starting points

Criminology refers as social control to mechanisms by which society ensures that its social norms are adhered to. It distinguishes between informal forms in the immediate environment, and formal social control, particularly through the police and criminal law. The category therefore includes things as diverse as rolling one's eyes at friends on the one hand, and imprisonment on the other. What all these mechanisms have in common,

1 The text was first published in Horst Beisel et al. (ed), *Die Kriminalwissenschaften als Teil der Humanwissenschaften: Festschrift für Dieter Dölling zum 70. Geburtstag* (Baden-Baden 2023) 963ff.

2 Alexander Armbruster, 'Er ist ein Star der künstlichen Intelligenz' *Frankfurter Allgemeine Zeitung* (Frankfurt, 22 March 2017) ‹https://www.faz.net/aktuell/wirtschaft/netzwirtschaft/andrew-ng-er-ist-ein-star-der-kuenstlichen-intelligenz-14936979.html› accessed 18 April 2024.

however, is that they are based on the concept of social norms and punish offences against these norms.

This backward-looking concept has come under pressure in the recent past. It is no longer enough for society to react to deviant behaviour in the past. Instead, the supposed ideal of comprehensive security has become dominant. To this end, violations of norms should be prevented, i.e., before they materialise in practice.[3] Society's response to theft, for example, has long been exclusively repressive and primarily left to criminal law. Of course, it would be more practical if such offences could be prevented in advance. Over time, a new, instrumental understanding of prevention and precaution has prevailed instead of what was characteristic of the welfare state of the postwar Federal Republic – from public safety measures and criminal prosecution to prevention, prediction and pre-emption.[4] It is not about changing social conditions and living circumstances in the sense of primary prevention, but about specific intervention regarding situations and persons to whom risks are attributed.[5] The central prerequisite for this idea is that potentially harmful situations and potentially dangerous people can be identified before the damage has occurred.[6] To this end, new forms of social control use the concept of risk. In short, this refers to a perceived potential for harm, and thus to circumstances that, statistically speaking, make the occurrence of harm or deviant behaviour more likely. For example, people are more likely to commit crimes when they are young than when they are older.

Artificial intelligence is a colourful term. It encompasses diverse techniques, such as machine learning, robotics, and neural networks. Therefore, artificial intelligence has many faces and is already being used in many different areas, such as online translation services, deepfake apps for manipulating videos, autonomous driving, drones, and weapons systems. However,

3 Tristan Barczak, *Der nervöse Staat* (Tübingen 2020); Tobias Singelnstein, 'Preventive Turn: Wie Gefahr und Risiko zum zentralen Gegenstand von Strafrecht und sozialer Kontrolle werden' in Thomas Fischer and Eric Hilgendorf (eds), *Gefahr* (Baden-Baden 2020) 96ff.

4 Uwe Volkmann, 'Prävention durch Verwaltungsrecht: Sicherheit' (2021) 40 NVwZ 1408, 1409ff.

5 Tobias Singelnstein and Karl-Ludwig Kunz, *Kriminologie: Eine Grundlegung* (8th edn, Bern 2021) 391ff.

6 General information on knowledge production in security law Benjamin Rusteberg, 'Wissensgenerierung in der personenbezogenen Prävention: Zwischen kriminalistischer Erfahrung und erkenntnistheoretischer Rationalität' in Laura Münkler (ed), *Dimensionen des Wissens im Recht* (Tübingen 2019) 233.

all of these are still quite simple forms, one could even say pre-forms of artificial intelligence in the true sense, and their interaction with the real world is often inadequate. There are machines that execute certain patterns for which they have been programmed, such as robots in industry. Programmes and algorithms can be trained with large amounts of data to recognise certain patterns, such as in autonomous driving. But we are still a long way from machines that actually act like humans, that can touch and grasp, that are able to deal with unfamiliar situations appropriately.

B. Artificial intelligence and social control

On the one hand, the technical developments described above pose new challenges and problems for the criminal sciences. In general, these automated processes raise the question of how negative consequences can be attributed. Who is responsible if, for example, an autonomously flying drone causes an accident? The new technologies also lead to new forms of crime, raising the question of whether they fall within the scope of existing criminal laws or whether new regulations are required.

However, AI also opens up new opportunities for social control.[7] For example, it can be used to make existing tasks easier: In the US, for example, predictive sentencing exists, which advises judges on their decisions, and automation is also finding its way into the administration of justice in Germany.[8] The police in Germany are developing tools to compare and identify handwriting or recognise sexual abuse of children in images; algorithms are designed to detect pattern-based money laundering, tax evasion or other economic crimes; upload filters by private companies on digital platforms recognise deviant behaviour and exclude it; video surveillance can identify

7 Overview at Alexander Baur, 'Maschinen führen die Aufsicht: Offene Fragen der Kriminalprävention durch digitale Überwachungsagenten' [2020] ZIS 275; Timo Rademacher, 'Verdachtsgewinnung durch Algorithmen: Maßstäbe für den Einsatz von predictive policing und retrospective policing bei Gefahrenabwehr bzw. Strafverfolgung' in Daniel Zimmer (ed), *Regulierung für Algorithmen und Künstliche Intelligenz* (Baden-Baden 2021) 234ff.

8 Martin Fries, 'Automatische Rechtspflege' [2018] RW 414; Johannes Kaspar, Katrin Höffler and Stefan Harrendorf, 'Datenbanken, Online-Votings und künstliche Intelligenz: Perspektiven evidenzbasierter Strafzumessung im Zeitalter von „Legal Tech"' (2020) 32 NK 35; Clemens Kessler, 'KI und Legal Tech. Utopie, Dystopie, Realität' in Susanne Beck, Carsten Kusche and Brian Valerius (eds), *Digitalisierung, Automatisierung, KI und Recht* (Baden-Baden 2020); Hannah Ofterdinger, 'Strafzumessung durch Algorithmen?' [2020] ZIS 404.

people – not only by means of facial recognition, but in the future, for example, also by the way they walk.

But AI is not just a tool. It also enables completely new forms of social control. By analysing patterns and correlations in crime data, it will supposedly be possible to predict deviant behaviour. Intelligent video surveillance can recognise behaviour patterns that are typical of dangerous or criminal behaviour, such as the hectic movements of several people in a dangerous place.[9] Prospectively, it is also expected to be able to interpret facial expressions in order to read motivations and attitudes such as an intention to buy, sexual interest, or suicidal intentions, or be able to recognise coronavirus infections.[10] Predictive policing – i.e., the prediction of criminal offences through mass data analysis – is still in its infancy in Germany. However, a look at the US demonstrates how influential the concept will be for police work in the future.[11]

These new technologies are not supporting already existing forms of social control, such as criminal law. Rather, they are taking their place as entirely new forms characterised by two features. Firstly, they follow a probabilistic perspective, i.e., they make probabilistic statements regardless of a specific occasion and well in advance of possible harm. This can be both person-related and situation-related. Secondly, they favour dealing with these risks in advance, which in turn can take various forms. On the one hand, this can consist of a more detailed investigation of the situation or the corresponding procurement of information. On the other hand, direct intervention in the respective event can be undertaken in order to achieve a change for the future, which is referred to as pre-emption.[12] Hence, these techniques claim to fulfil social control's long-held desire – namely, to prevent deviance. In the case of theft, it would no longer be necessary to wait for the offence to be committed. Instead, the facial expression or other social characteristics of potential perpetrators could be used to recognise whether they are more likely to commit theft.

9 Sebastian J Golla, 'Lernfähige Systeme, lernfähiges Polizeirecht. Regulierung von künstlicher Intelligenz am Beispiel von Videoüberwachung und Datenabgleich' (2020) 52 KrimJ 149, 156f.

10 Wolfgang Behr, 'Gesichtsverlust 3.0' (*Geschichte der Gegenwart*, 18 April 2021) ‹https://geschichtedergegenwart.ch/gesichtsverlust-3-0/› accessed 18 February 2022.

11 Tobias Singelnstein, 'Predictive Policing: Algorithmenbasierte Straftatprognosen zur vorausschauenden Kriminalintervention' [2018] NStZ 1, 2ff.

12 Simon Egbert, 'Drogentests und 'Alltags-Präemption'' (2018) 50 KrimJ 106, 109ff.

C. Problems and question marks

The way of dealing with risks as exemplified by these new techniques of social control can be divided into three abstract steps: Calculation or identification, assessment, and management.

I. Risk identification

At the level of risk identification or calculation, the aim is to determine factors that make the occurrence of deviant behaviour more likely for certain people or situations.[13] The systems operate according to the principle of pattern recognition. In a first step, vast data sets are examined to see whether certain patterns can be identified that are associated with deviant behaviour. This can refer to various things. On the one hand, very specific things, such as certain behaviour or a certain facial expression in the case of intelligent video surveillance. On the other hand, there are also comprehensive procedures, such as in the case of predictive policing systems, which create profiles of people or analyse situations using a wide range of different data. If patterns are identified that statistically make the commission of criminal offences more likely, the systems are trained to recognise them in the real world so that they can be evaluated and managed there.[14]

In this way, AI opens up interesting new perspectives. Under certain circumstances, it can even provide insights that were previously hidden from us, as human behaviour can be measured and calculated to a certain extent, thereby leading to a new understanding of risk.[15] However, risk identification in the area of social control of deviant behaviour is also associated with fundamental difficulties, in particular our incognizance of risks which impedes the clear definition of patterns. Firstly, human behaviour is only measurable and predictable in some respects; if there are patterns to varying degrees, some risk factors are easier to predict than others. Secondly, the quality of pattern recognition depends heavily on the complexity of the subject in question.

13 Tobias Singelnstein and Karl-Ludwig Kunz, *Kriminologie: Eine Grundlegung* (8th edn, Bern 2021) 394ff.

14 Mareile Kaufmann, Simon Egbert and Matthias Leese, 'Predictive Policing and the Politics of Patterns' (2019) 59 BritJCrim 674.

15 Kelly Hannah-Moffat, 'Algorithmic risk governance: Big data analytics, race and information activism in criminal justice debates' (2019) 23 Theoretical Criminology 453.

Finally, these processes require the collection and processing of (also) personal data on a very large scale.[16] Firstly, large amounts of data are required for the techniques to train and work with, for example in order to recognise patterns – the more and the more diverse the data, the better. Secondly, once these technologies are functioning, they will have to constantly survey us and our world in order to detect patterns and risk factors.[17] The more comprehensive this preventive surveillance is, be it through video surveillance or data analyses, the more the technologies can discover.

Due to the intrusive nature of such measures with regard to informational self-determination, approaches that look at situations and therefore do not process personal data have dominated in Germany to date. However, forms of personal risk analysis are also increasingly entering the scene.[18] These are currently still focused on certain groups, such as multiple offenders, sex offenders and dangerous offenders, working primarily with existing police databases and not yet using AI, as shown by police databases, but also by the BKA's RADAR programme (rule-based analysis of potentially destructive offenders to assess the acute risk).[19] However, various projects, particularly from the BMBF's security research programme, show where the journey is heading: data-based, automated risk analyses, including those relating to individuals. This can be based on very different data sets, including those from social media.[20]

II. Risk assessment

The issue becomes much more difficult when it comes to assessing the respective risks, i.e., the question of what the existence of a risk factor actually means in concrete terms and what the consequences should be.

16 Simon Egbert, 'Datafizierte Polizeiarbeit – (Wissens-)Praktische Implikationen und rechtliche Herausforderungen' in Daniela Hunold and Andreas Ruch (eds), *Polizeiarbeit zwischen Praxishandeln und Rechtsordnung* (Wiesbaden 2020).

17 Hans-Heinrich Kuhlmann and Simone Trute, 'Predictive Policing als Formen polizeilicher Wissensgenerierung' [2021] GSZ 103, 108f.; see also Sebastian J Golla, 'Lernfähige Systeme, lernfähiges Polizeirecht. Regulierung von künstlicher Intelligenz am Beispiel von Videoüberwachung und Datenabgleich' (2020) 52 KrimJ 149, 157f.

18 Lucia M Sommerer, *Personenbezogenes Predictive Policing* (Baden-Baden 2020).

19 Celina Sonka and others, 'RADAR-iTE 2.0: Ein Instrument des polizeilichen Staatsschutzes: Aufbau, Entwicklung und Stand der Evaluation' [2020] Kriminalistik 386.

20 Michael Spranger and Dirk Labudde, 'Vorhersage von Gruppendynamiken auf der Grundlage von Daten aus Sozialen Netzwerken' in Thomas-Gabriel Rüdiger and Petra Saskia Bayerl (eds), *Cyberkriminologie* (Wiesbaden 2020).

Here, the new techniques of social control, like all forms of forecasting, have to contend with the problems of ambivalence, complexity, and uncertainty. These are particularly evident in the prediction of deviant behaviour. For not only is deviant behaviour highly diverse, but it also involves very complex social events that can be influenced by a large number of very different factors.

Whether and why someone violates social norms depends on countless factors, some of which exert their influence in the long-term and others spontaneously. There are now myriad criminological theories explaining the development of crime in one way or another. Depending on their epoch and the paradigm in force, they seek the causes of deviance in disposition or environment, in biological, psychological, social or socio-structural circumstances. Yet we really only know of certain factors that make the occurrence of deviant behaviour more likely. There is no universal formula to explain criminal behaviour.[21] And while it is one thing to attempt to theoretically and empirically clarify how crime arises, the prediction of deviant behaviour by certain individuals in concreto is something completely different. Even in the field of crime prediction, which involves a very specific population of test subjects or very specific issues, the methodological possibilities of predicting future criminal offences are highly controversial and anything but satisfactory.[22]

However, once someone has been identified as a dangerous offender, it is difficult for them to exculpate themselves, to free themselves of this label. Where there is no specific accusation but only a vague assessment, it is impossible to convincingly exonerate oneself. The European and international no-fly lists have impressively demonstrated how Kafkaesque this can become.

III. Risk management

The third step involves the question of how to deal with the risks that have been identified and assessed. There are various possible forms for this. On the one hand, there are so-called recommender systems. These provide information and recommendations on how a certain situation should be

21 Tobias Singelnstein and Karl-Ludwig Kunz, *Kriminologie: Eine Grundlegung* (8th edn, Bern 2021) 219ff.

22 See only Ulrich Eisenberg and Ralf Kölbel, *Kriminologie* (7th edn Tübingen 2017) 228ff.

handled, but do not make decisions themselves. These include predictive sentencing systems, for example, which are designed to support judges in their decision making. For such systems, the question always arises as to what extent the decision-makers remain capable of making qualified assessments for themselves and, if necessary, of resisting the recommendations. On the other hand, systems can incorporate automated decisions, for example when an intelligent video surveillance system triggers an alarm or locks rooms.

There are also various ways of managing risks. Firstly, concrete control, i.e., intervention to handle a specific risk situation, can be considered. This handling could consist of risk research, for example by ordering police officers to a certain location where the probability of burglaries is said to be increased, or by observing potentially dangerous people to obtain further information about them and their actions and to clarify whether a threat is materialising. However, it is also possible to directly modify the risk situation. For example, a potential thief could be denied access to a department store if the video surveillance identifies a suspicious facial expression.

Secondly, there are precautionary models that link more or less comprehensive consequences to more general risk predictions. The aim then is not to deal with specific identified risks, such as an increased probability of burglary or theft. Instead, the general riskiness of people is determined in the form of risk profiles using a large number of parameters in order to link them with an equally broad range of reactions in terms of prevention. What this might look like in practice is demonstrated by glimpses of China's notorious social scoring system[23] – or the private sector. In Germany, too, SCHUFA and insurance companies have long been using social scoring to assess creditworthiness or the probability of insurance claims.[24] In the case of SCHUFA, this form of risk management can lead to someone being unable to obtain credit (or only at very expensive rates) or enter into certain contracts. The Chinese social scoring system, for example, excludes people from buying tickets for flights and train journeys once they reach a certain score. By these measures, an increased, not necessarily further specified risk profile is dealt with before these risks materialize any further.

23 Katika Kühnreich, 'Social Credit, Sicherheit und Freiheit' in Oliver Everling (ed), *Social Credit Rating* (Wiesbaden 2020).

24 See also Niklas Maamar, 'Social Scoring: Eine europäische Perspektive auf Verbraucher-Scores zwischen Big Data und Big Brother' (2018) 34 CR 820, 820ff.

At the same time, however, such forms of precautionary exclusion obviously also constitute sanctions and therefore incentives for good behaviour and self-management. These incentives do not necessarily have to be of such an overt nature but can also take on a manipulative form. AI and algorithms offer excellent opportunities for this, as they are getting to know us better and better and can not only predict our behaviour and decisions, but are also aware of our needs, desires, and fears.[25] From a technical point of view then, the step to risk management through manipulation is not too far away.

So, while we can observe different techniques, their underlying principle is the same: risk management. From this perspective, governmental social scoring ultimately appears to be merely a logical further development of the techniques already used in Germany today.

D. The security of the future

The technologies and strategies described in the context of AI will lead to a fundamentally different image of deviant behaviour and crime – and thus create a fundamentally different social understanding of security. Security is a social construct. Its form and change are characterised by the respective social conditions and existing social discourses. How much security is necessary? Regarding which areas and topics? Whose perspective is decisive? What exactly does security mean – i.e., when is it present and when is it disturbed? These questions are answered differently at different times and in different societies, but also by different groups in society. Central to this issue is what a society sees as disruptions and threats, i.e., what its sources of insecurity are and which concepts are favoured in dealing with them.

I. Disruptions to the security of the future

In future, the things that are conceived as disruptions to security, as sources of insecurity, and as threats will be very different from today. The focus will

25 'Gefahr für die Menschheit: Vordenker warnt vor möglicher Macht der Algorithmen' (*Chip*, 9 May 2019) ‹https://www.chip.de/news/Gefahr-fuer-die-Menschheit-Vordenker-warnt-vor-moeglicher-Macht-der-Algorithmen_168085191.html› accessed 18 April 2024.

no longer lie with crime and behaviour that deviates from social norms, as is the case today with criminal law and related techniques of social control. Instead, risk factors (as they are addressed and dealt with by the new AI techniques of social control) will already be seen as disruptions to security by themselves.[26]

According to this way of thinking, a normal person is not someone who merely refrains from prohibited behaviour, but someone who possesses no risk factors for future deviant behaviour. In the world of probabilistic perspectives, the predictability of risks becomes the decisive question. These techniques – and therefore we ourselves – will no longer look at whether people's actions violate norms, which requires a very precise determination. Instead, they calculate probabilities of a possible norm violation in the future and consider this risk factor as a disruption well in advance of any harm. From this perspective, it follows that we no longer look at individual actions of people and assess them, as we have done in criminal law to date. Instead, we look at people and situations as such and subject them to a forward-looking overall assessment when analysing risk. In the case of individuals, this introduces the possibility of rating, i.e., categorising the population into different risk classes. Let's think back to the example of theft: a thief does not only come into focus when he commits the theft, but already when he enters the department store with a suspicious facial expression or otherwise exhibits risk characteristics that speak in favour of committing theft – young age, wrong residential area, previous criminal record. This may be practical regarding a person who actually wants to commit theft. However, it also applies to dozens of others who have similar risk characteristics but would not actually commit theft. The techniques do not judge individuals as such, but construct groups based on probability statements.

The changed understanding of security disruptions will bring completely different phenomena to the centre of attention. Which forms of disruption are at the centre of social perception and how they are understood always depends on the respective strategies through which a society endeavours to control these disruptions. For example, repeat offenders only became an issue when police files and forensic evidence made it possible to prove that individual suspects had committed several offences. Where predictions

26 Kelly Hannah-Moffat, 'Algorithmic risk governance: Big data analytics, race and information activism in criminal justice debates' (2019) 23 Theoretical Criminology 453.

are made based on pattern recognition, as is the case with AI, the focus naturally shifts to disruptions that exhibit certain patterns. And society's perception will focus more on external signs of such patterns than on attitudes, social explanations, and similar causal contexts.[27] In criminology, other theories of crime that follow this pattern-based, external perspective will become stronger.

However, this fundamental change does not – as one might perhaps hope – mean that there will no longer be any disruptions to security. Rather, only the understanding of what is to be regarded as a disruption is changing – namely the risk factor well in advance of actual harm or violations of legal interests.

II. Dealing with disruptions to the security of the future

Dealing with disruptions to security – i.e., calculating, assessing, and managing risks – is to a large extent the state's responsibility and primarily the task of the police. At the same time, however, the new understanding also shapes the practical experiences of citizens. In their everyday lives, they endeavour to recognise risks and take precautions to counter them. Police prevention programmes even encourage them to do so. Today, more than in previous decades, protection against threats and concern for security are also projects of the individual. After all, the production of security is increasingly becoming a market. Private companies offer their own solutions for calculating and assessing risks as well as corresponding precautionary measures. In doing so, they further stimulate both public and private risk management.

Looking outward from today's perspective, it is difficult to say which proportions this risk management will assume in society. It is conceivable that this management will extend only to particularly significant risks. If sufficiently concrete patterns and risk factors for homicides could be identified, these could be countered with selective control through risk research measures. At the other end of the scale looms the model of comprehensive risk management favoured in China: By comprehensively surveying the world, people, and their actions through intelligent video surveillance and various data analyses, a permanent calculation of risks is taking place, and

27 Tobias Singelnstein, 'Predictive Policing: Algorithmenbasierte Straftatprognosen zur vorausschauenden Kriminalintervention' [2018] NStZ 1, 4f.

they can be assigned to individuals by way of already ubiquitous facial recognition.[28] Here, identification and risk detection as different areas of application for AI are therefore linked. In the preventive model, the necessary management is implemented in the form of a social credit system.

In Germany and Europe, the direction of development will depend heavily on whether society succeeds in dealing rationally with relevant risk factors. After all, risk factors are defined precisely by the fact that they only provide for a statement of probability and do not always materialise. However, there is little cause for optimism in this respect. This is not only demonstrated by the way we deal with security incidents and crime today, which is often not very rational or evidence based. The findings of research being done on risk acceptance also suggest that our society will find it extremely difficult to react rationally, since these risks have practically everything that makes them particularly unacceptable: they are not taken voluntarily, but are imposed; they are difficult to control and usually have no positive benefits, but may have serious consequences and potentially affect all or many people.[29] And the expectation of prevention associated with this is almost never-ending, never sufficient, can always go even further, is always possible even earlier and always finds even further risk factors.

E. Conclusion

Artificial intelligence technologies offer new possibilities and the opportunity for innovative insights within the field of social control. They promise to do almost exactly what was previously impossible. At the same time, however, they also harbour massive problems and raise fundamental questions. Firstly, we can only inadequately calculate and assess the risks of future deviant behaviour – at least from today's perspective. Such techniques will therefore primarily reproduce existing images of criminality with all

28 Madeleine Genzsch, 'Harmonie durch Kontrolle? Chinas Sozialkreditsystem' in Tobias Loitsch (ed), *China im Blickpunkt des 21. Jahrhunderts* (Berlin/Heidelberg 2019) 136ff.; Wolfgang Behr, 'Gesichtsverlust 3.0' (*Geschichte der Gegenwart*, 18 April 2021) ‹https://geschichtedergegenwart.ch/gesichtsverlust-3-0/› accessed 18 April 2024.

29 Michael Zwick, 'Risikoakzeptanz und Gefahrenverhalten' in Thomas Fischer and Eric Hilgendorf (eds), *Gefahr* (Baden-Baden 2020) 40ff.

their distortions.[30] Where do the ethical limits lie for such AI? How can effective control and legal regulation of such algorithms be organised? Is calculating and surveying really superior to chance?

Secondly, this means that AI is acting as a motor for fundamental change in social control, which is now increasingly focussing on the management of risks in order to prevent potential harm in advance. Taken together, this will shape the security of the future, i.e., our image of security, disruption, and insecurity, and how society should deal with them. Security in this sense is becoming increasingly important. It is increasingly being framed as an ideal of absolute security. And it appears as a security constantly under threat in the face of risks – which, from a subjective point of view, creates uncertainty rather than security, resulting in a permanent loop. Where are the limits of such developments, such a constant shift forward?

Thirdly and finally, the change described and these strategies of risk management are associated with extremely problematic consequences, namely with chilling effects: the more comprehensively risk recognition and risk management are designed as forms of social control, the greater the pressure on the individual to behave in a compliant manner and not to attract attention. On the one hand, this gentle restriction of autonomy and freedom without coercion may be efficient. On the other hand, however, it is also dangerous precisely because it is less conspicuous and avoids societal debate. Where do the absolute limits for these forms of influence and manipulation lie in a democratic constitutional state? To what extent are our contemporary dogmatics, and constitutional law in particular, capable of preserving these limits in practice – especially considering the powerful image of the security of the future that is beginning to emerge?

30 Jan Wehrheim, 'Definitionsmacht und Selektivität in Zeiten neuer Kontrolltechnologien' in Henning Schmidt-Semisch and Henner Hess (eds), *Die Sinnprovinz der Kriminalität* (Wiesbaden 2014).