MAKING SURVEILLANCE PUBLIC

WHY YOU SHOULD BE MORE WOKE ABOUT AI AND ALGORITHMS

Marc Schuilenburg

eleven

'A cogent, crisp, and convincing book on the challenges brought by AI and big data applications with respect to crime control and security'
Gary T. Marx, author of *Undercover* and *Windows into the Soul*

'*Making Surveillance Public* powerfully charts a path forward for examining the digitalisation and algorithmisation of surveillance and its effect on criminology'
Chris Gilliard, writer for *Vice, Wired, Real Life Magazine* and *The Atlantic*

What are the new questions raised by AI for the prevention and detection of crime? How can we rationalise the Amazon Ring doorbell and Tesla's Sentry Mode? How can algoracism be identified, and what should we think of data donation?

Surveillance today cannot be understood without an awareness of how AI and algorithms have become increasingly central in the governance of security. They have led to a substantial expansion in the depth and breadth of surveillance, ranging from mass data collection to mass invasion of privacy. In *Making Surveillance Public*, Marc Schuilenburg explores the deployment of AI applications, asking who is using them, what their aims are, what outcomes and societal impacts they lead to, and against whom they are used. To this end, he makes a case for a digital criminology centred on sociological questions of power, knowledge and AI experiences.

Marc Schuilenburg is a Professor of Digital Surveillance at Erasmus University Rotterdam. Schuilenburg's other works available in English include *Hysteria, The Securitization of Society* and *Mediapolis*.

ISBN 978-90-4730-205-6

Making Surveillance Public

MAKING SURVEILLANCE PUBLIC

WHY YOU SHOULD BE MORE WOKE ABOUT AI AND ALGORITHMS

Marc Schuilenburg

eleven

Published, sold and distributed by Eleven
P.O. Box 85576
2508 CG The Hague
The Netherlands
Tel.: +31 70 33 070 33
Fax: +31 70 33 070 30
e-mail: sales@elevenpub.nl
www.elevenpub.com

Sold and distributed in USA and Canada
Independent Publishers Group
814 N. Franklin Street
Chicago, IL 60610, USA
Order Placement: +1 800 888 4741
Fax: +1 312 337 5985
orders@ipgbook.com
www.ipgbook.com

Eleven is an imprint of Boom (Den Haag).

Book cover design and AI Images by IJzersterk.nu (with Adobe)
Translation by Vivien D. Glass and Anna Asbury
Design inner work by Textcetera

ISBN 978-90-4730-205-6
ISBN 978-94-0011-392-3 (E-book)

'It's never the code's fault,' says T-Li.
'Even when it is.'

Charles den Tex – *Bot* (2016)

Table of Contents

1 The Problem Field

1.1 Introduction

What do the Amazon video doorbell Ring, Tesla's electric cars and the Waze navigation app have in common? At first glance not much, other than all being consumer goods that come with a substantial price tag – at least in the case of Tesla and Ring. The American tech company Amazon introduced the smart doorbell Ring to the market a few years ago. This doorbell enables users to see who's at the door. It works over Wi-Fi and when someone presses the bell, they appear on the owner's smartphone or tablet, allowing the user to decide whether or not to let them in. In the most expensive version of the digital doorbell, filming starts a few seconds before the person rings the bell – as someone rides up on their bike, for instance, or walks up the garden path to the front door.

Tesla's electric cars have a similar monitoring system installed, known as Sentry Mode. This function uses the car's inbuilt cameras not only to record the owner's driving, but also to check the area outside the car for suspicious movements. It

makes use of the latest technology to identify people who want to damage or break into the Tesla. When these people come into view on the cameras, the owner receives a warning on the Tesla app. This is intended to protect the car against theft or vandalism.

Users of the popular navigation app Waze receive real-time traffic information as to how busy the roads are, but also how to get to the destination without driving through a 'higher crime risk area'. Waze is the property of Google and the app includes the function 'Avoid high risk areas' which advises drivers to avoid dangerous neighbourhoods, even if they are on the quickest route.

The Ring doorbell and Tesla's Sentry monitoring system are examples of what Chris Gilliard and David Golombia (2021) have termed 'luxury surveillance' – products for which people are prepared to pay a great deal of money because their presumed advantages, in preventing crime and monitoring oneself, are seen as positive characteristics. A similar monitoring system can be found in the e-bikes of the futuristic bicycle brand VanMoof, with an average price of more than 3,000 euros. When cycling, the motor sensors send speed information to your phone, and the associated app sends these on to the company's servers to calculate your journey time and distance, among other things. Luxury surveillance differs in this respect from externally imposed surveillance: surveillance that the subject would rather not have but is required for some reason. The latter case might include electronic monitoring by means of an ankle tag, a kind of Apple Watch for prisoners, allowing

detainees to spend their sentence outside prison walls because a transmitter on the tag allows staff to check their whereabouts at all times.

Aside from the substantial price tag and voluntary purchase by wealthy individuals, luxury surveillance is characterised by the imperatives of surveillance capitalism: customers are tied to private tech companies by an app, and large quantities of personal data are collected and unlocked using algorithms, one of the aims being to make society safer. For instance, the recorded images from the Ring Bel and the Sentry monitoring mode are not only shared with other individuals on Amazon and Tesla's online platforms; users of these digital saviours also receive automatic notifications of 'suspicious' activity in their street or around their Tesla.

1.2 What is surveillance?

The word *surveillance* comes from Latin and French. The Latin word *vigilāre* means 'to keep watch' or 'to guard'. The French word *surveiller* means 'to keep watch over' and 'to monitor' (*veiller*) 'from above' (*sur*). The term has been used in English since the nineteenth century in the sense of 'keeping an eye on' things, which invokes a range of different activities that tend to be viewed as synonymous, from inspecting and examining to observing individuals.[1] These are human actions that often take place in a secretive and unnoticed manner rather than being visible to the general public, and in which the individuals monitored form a passive object of control. This

'monitoring' was initially carried out with the naked eye, with a clear distinction between the person watching and the individual being watched. This physical form of surveillance was extremely labour-intensive and relatively little information was stored. Gary Marx (2016) terms this 'traditional surveillance'.

Political scientists such as James Scott (1999) and Anthony Giddens (1984) have shown that with the rise and expansion of the nation state, surveillance activities have increasingly come to revolve around collecting information to serve the purpose of governing society. Intensified monitoring of the population in various domains of society, including work, school and in prisons, is seen as necessary in order to better govern this territory and is thought to guarantee greater prosperity and well-being. Giddens defines surveillance as 'the coding of information relevant to the administration of subject populations, plus their direct supervision by officials and administrators of all sorts' (1984: 183).[2] Kevin Haggerty and Richard Ericson base their reasoning on the same rationale of governance and describe surveillance as 'the collection and analysis of information about populations in order to govern their activities' (2006: 3). Western governments began to conduct population censuses in the nineteenth century, the results being entered into registers by hand in a standardised format, which made a more detailed view of the lives and living conditions of the population available. The recognition and registration of a country's residents makes the society, in the words of Scott (1999), 'legible' – and therefore also malleable, controllable and governable.[3]

From the beginning, surveillance has had negative connotations for many people. It invokes the dystopian image of a totalitarian regime, of a state or sect wanting to know everything about its citizens and using surveillance for monitoring and guarding the population. Media suggestions that we are sleepwalking into a digital surveillance state or surveillance dictatorship contribute to this view. The surveillance state is seen as a contemporary expression of a sovereign power, a negative conception of power that is repressive by nature and is used to determine what is permitted and what is not.[4] This power is exercised from above and with its long information tentacles reaches all corners of society – its main goal being to control every aspect of daily life. China is the nightmare scenario. The media often refer to the Leviathan-like omnipotence of the Chinese state, where Big Brother and Big Data come together in a national social credit system, scoring citizens based on high-volume data collection in order to express their level of 'trustworthiness'. Anyone in China who runs a red light, gambles or has a criminal record can be excluded from things like jobs, accommodation or loans. The fear of such developments is understandable. No one feels comfortable with being constantly watched by technical gadgets like drones, smart cameras and sensors, or being ranked as an A-, B-, C- or D-citizen, particularly if this happens unchecked and on a large scale, with the potential for exclusion from certain rights or from access to particular amenities.

It is also precisely this image of deep and ubiquitous oversight and monitoring that was the first major stimulus for scientif-

ic research into the role surveillance plays in Western societies and what its consequences are, intentional or otherwise.

1.3 Research into surveillance: three phases

In the early 1990s the question of what surveillance was and how it worked in practice led to research, particularly in Anglo-Saxon countries, into the ways in which physical forms of monitoring had been taken over by a growing collection of surveillance cameras – on the street, in shopping centres, on aeroplanes and on public transport (Galič, Timan & Koops, 2017). The assumption here is that the spy cameras have a disciplining effect and that social problems such as rising crime and antisocial behaviour can be better tackled this way. The research also pointed to the related negative effects of recognition and registration by camera monitoring, including what is termed a 'chilling effect': individuals do not feel completely free and behave differently when they believe they are being watched, regardless of whether this is actually the case (Fussey & Murray, 2019; Murray et al., 2023).

An important stimulus behind this initial phase of research into surveillance was Michel Foucault's book *Surveiller et punir* (1975), in which he describes the emergence of a disciplinary form of power in the seventeenth and eighteenth century that steers people in the direction of socially responsible behaviour by making them into productive, efficient and obedient individuals. The actualisation of this new power relationship takes place in schools, barracks, factories, hospitals and prisons

– Foucault names these modern institutions 'disciplinary practices' – where various methods (dressage, timetables, exams, exercises) are applied to the bodies of those present in order to discipline and drill them. The disciplining of prisoners, labourers, the mentally ill and school children is not a uniform process, but the result of a whole series of effects that reinforce one another. Each separate institution finds its own way of integrating the new power relationship into its specific environment in order to achieve socially desirable behaviour. Foucault intended his analysis to be distinct from more everyday conceptions of power, such as the notion that power is the property of an individual (a monarch, for instance) and – in particular – from notions of power in legal discourse and Marxism, where it is described in terms of law ('prohibition') and subjugation ('sovereign power'). Foucault believed that power should not be seen as purely negative, but that it can also be productive, because it gives rise to a reality that is expressed in normative discourse and disciplinary practices. The most famous example of this is the prison model of the Panopticon.

Panopticon, a Latinisation of the Greek πανόπτης (*panoptēs*), meaning 'all-seeing', refers to the model of a prison designed by the famous British philosopher Jeremy Bentham, a circular building with a watch tower in the middle that offers the guards a view through blinded windows into the individual cells inside the ring. Even when no guard is present in the tower, the prisoners continue to feel spied on, as if they have effectively internalised the monitoring, adjusting their behaviour to what they believe is expected of them ('normalisation'). This leads to a notion of 'panoptic surveillance', whereby monitoring is

centralised and permanent observation is possible without the prisoners being able to tell whether they are seen or by whom. Foucault talks here about 'docile bodies' – people made pliable, controllable and recognisable with the use of technology. You could also say that the power of panopticism lies in the fact that the people who are watched start to engage in a form of self-surveillance.

A second important stimulus for research into surveillance in society came from an article by Gilles Deleuze with the title *Post-scriptum sur les sociétés de contrôle*, which appeared in 1990 in the French publication *L'Autre journal*. In this article he makes the point that the disciplinary society described by Foucault is slowly shifting to become a control society. Objectifying techniques that read and train people have taken on a technological character, enabling control to become distinct from the seclusion of specific institutions of the past. In doing so, control replaces internalised disciplinary power and becomes a permanent process. Deleuze writes: 'The conception of a control mechanism, giving the position of any element within an open environment at any given instant (be it animal in a reserve or human in a corporation, as with an electronic collar), is not necessarily one of science fiction' (1990). This means that the control society no longer works via closed, fixed spaces (the walls, borders or gates of prisons or factories), each with their specific function, but operates through ever-changing, constantly interacting networks. Mobility, flexibility and acceleration are the primary characteristics of these networks, incorporated into the surveillance literature with concepts such as the 'surveillance web' (McCahill, 2002) and 'surveillant

assemblage' (Haggerty & Ericson, 2000; 2006; Ericson 2007). Other terms that regularly crop up on this theme are 'postmodern surveillance' (Staples, 2000) and 'rhizomatic surveillance' (Bogard, 2006).

Research into the second phase of the history of surveillance focuses primarily on actuarial and preventative forms of monitoring, the most familiar example being CCTV (Closed Circuit Television) in the United Kingdom. It allows users to follow the movements of individuals over a long distance and time period through a network of thousands of cameras in order to prevent crime and antisocial behaviour due to the potential deterrent effect of cameras, and by using the images retrospectively as evidence or to take action if an incident is observed.[5] A pertinent difference between CCTV and traditional camera monitoring is that the video connection now happens over a closed circuit or network. It is also possible for public and private parties to collaborate here, so that operational management is carried out by the police, local council or a private security company – or a combination of these parties.

In just a decade, our society has entered the era of big data and algorithms and this has led to the third – and most recent – period of academic research into surveillance. David Lyon states that 'surveillance today cannot be understood without a sense of how the quest for "big data" approaches are becoming increasingly central' (2015: 68-69). Big data is generally described as having four main technical characteristics: it involves very large *volumes* of data, this data is collected at high *velocity*, the data is unstructured and *varied*, and it is

digital (Laney, 2001; Gartner, 2011).[6] Big data is unlocked by algorithms, which come in various different types, from simple applications such as decision trees and data exchange systems to technically extremely complex applications, such as machine learning and variants on this such as deep learning (or a combination of the above). When people talk about Artificial Intelligence (AI) they often mean complex applications of this kind, in particular systems with the capacity to learn independently and make decisions. This also comes up in the definition of AI used by the European Commission's High-Level Expert Group on Artificial Intelligence: 'Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals' (2019).[7]

Continuing the example of the security cameras: with AI, the camera can now be equipped with sound analysis and automatic facial recognition technology. In this form of biometrics, the images from the camera are compared with images of individuals stored in an enormous database, from detainees and convicted criminals to asylum seekers and football hooligans. For instance, Dutch football stadiums are experimenting with smart cameras equipped with sound sensors that make it possible to follow and identify supporters close up throughout the match, recording an individual audio file for each supporter, in order to judge whether anyone has crossed the line in speech or song, for instance by making racist noises.[8] Another example is the 'Operationele Proeftuin Roermond', a testing ground at the outlet shopping centre in the city of Roermond in the south of the Netherlands. A couple of years ago the police started up

a project known as the Sensing-project here to avoid mobile banditry. Smart cameras and sensors are set up in various spots to register the number plate, make and model of passing cars and to record what route they took. Algorithms then calculate whether a vehicle should be regarded as 'high-risk'. If so, an alarm sounds in the control room and the police can follow the car and check on those inside. This kind of smart camera monitoring is still in its infancy, yet people are already talking about 'algorithmic surveillance' (Norris et al., 1998; Murphy, 2017; Kosta, 2022).

1.4 Theoretical frameworks and empirical research

Over the last few decades, a completely new infrastructure has arisen in our society, one we never encountered before and with which we must learn to live. You could say that surveillance has become fluid and continuous, with digitalisation through AI and algorithms compounding the situation. Whether we're talking about the Amazon Ring doorbell or Tesla's Sentry Mode – in which cameras record everything and monitor the surroundings for suspicious activity – social media following our online lives and transmitting our personal preferences, lifestyle apps to make life easier by remembering the shopping and providing insight into your health, or public parties such as local councils and the police, who are interested in predicting and preventing risky behaviour, surveillance by means of AI and algorithms determine the way in which our society functions. It is worth noting here that surveillance in this sense does not so much serve its original purpose of 'keeping an eye on things'.

Its meaning has slowly changed into 'making things visible' (Taylor, 2017; Harcourt, 2007; 2015) which happens through high-volume data collection for analysis and interpretation and subsequently leads to decisions and concrete action, for instance monitoring in the right place for the threat of crime. Another difference from traditional surveillance is that all this no longer has to happen through human activity, as it can be conducted entirely automatically and autonomously.

The theme of 'surveillance' has never taken up much space in criminology. This is remarkable, given that developments in this area are always closely connected with the government and other parties' approach to crime and antisocial behaviour. The process requires recognition and registration of individuals who are regarded as high-risk or who need protection (De Graaf, 2013). There has so far been very limited academic research into surveillance methods in policing and the evidence base for their efficacy in preventing and detecting crime. What's more, recent private phenomena such as the Amazon Ring doorbell and the monitoring functions in Tesla's electric cars have not caused much of a stir, nor have they set alarm bells ringing in the field of criminology.[9] Nevertheless the use of technology by foreign tech companies is anything but an innocent exercise. The Amazon Ring, for instance, is more than just a doorbell. It also functions as a security camera that records images throughout the day, which the users can later view and share with others and the police. The doorbell can even potentially work as a microphone, recording voices and other noises at the door, from the neighbours and in the street. This gives rise to a completely new surveillance circle to make neighbour-

hoods safer, compounding issues around the relationships and boundaries between private and public interests. On this subject, the American company speaks of 'The New Neighbourhood Watch', but what are the consequences of this in terms of security? Does the digital doorbell lead to a drop in the number of burglaries? Is it desirable that both Amazon and the police can see everything that goes on around the house? This also raises a number of complicated legal issues, such as where private space ends and public space begins.

It is problematic that in criminology, theoretical and normative frameworks as to how to approach AI in relation to security are unclear or even completely absent. This applies in such areas as the government's handling of tech companies that constantly collect and analyse data, using it both to monitor and influence citizens. This results in the distribution of fake news to sway elections, polarisation that can lead to extremist thinking and radicalisation, exploitation of users' psychological states with results such as addiction, and emotional manipulation with instigation to suicide as the most extreme example. All of these are criminal offences punishable by prison sentences. Normative principles tailored to the vulnerabilities of the use of AI applications in security are also thin on the ground. The use of new surveillance technologies is often paired with lofty and unrealistic expectations as to the benefits of technological applications, without a critical look at the consequences for public values relating to fundamental human rights: from a dearth of accountability processes around the use of algorithms and stigmatisation of certain groups to unequal power relationships between public and private parties.

There have so far also been very few robust empirical studies into the effects of AI applications, and the scarce evaluations we do have, in this case on predictive policing, have shown contradictory and varying results. In a number of American cities the implementation of predictive policing turns out to have been effective, while in other countries, including the Netherlands, there is no demonstrable effect on crime (Mohler et al., 2016; Mali, Bronkhorst-Giesen & Den Hengst, 2017; Meijer & Wessels, 2019; Ratcliffe et al., 2021). Enthusiastic and positive stories about AI turn out often to be based on anecdotal evidence or to derive from 'corporate storytelling' by tech companies with the aim of selling such applications to governmental organisations or of processing and analysing the data themselves, which can in turn lead to societal risks such as 'vendor lock-in' (Zuboff, 2019; Slobogin & Brayne, 2022).[10] It is rare to see research into whether the application actually works ('what works') or whether the way it works ('how it works') is commensurate with the results. After all, the simple fact that something is possible does not necessarily make it desirable. Does the purpose of an AI application weigh up against the added value of other solutions, for example? What if we have far simpler and more human solutions right in front of our noses? All this leads to a knowledge and power vacuum which raises the question what price is being paid for it, both in scientific terms and in its effect on society.

1.5 The question

What I would like to investigate, based on these introductory observations, is the way in which security is changing due to the rise of different forms of AI applications. To what extent does AI raise new questions with respect to the prevention and detection of crime and antisocial behaviour? And how far-reaching are the consequences for society in general and criminology in particular? The translation from traditional physical 'watching over' the safety of citizens by the police to digital methods of surveillance by a plethora of public and private bodies has, after all, hardly been tested in criminological research. The academic literature presents a void on this point which in my view requires filling.

The problem of AI is so broad, and the scale and variability in digital applications so overwhelming, that it is necessary to zoom in on a specific context. The security domain involves countless issues relating to AI, from the substantial increase in cybercrime and the use of algorithms to advise judges on a suspect's risk of recidivism to the enforcement of sentences (electronic ankle tags). I demarcate my research in particular by focusing on the phenomenon of big data policing: the use of large volumes of structured and unstructured data unlocked by algorithms with the aim of making society safer and more liveable. Questions I would like to ask on this topic are: how can society benefit as much as possible from this? But also: how can ethics and the rule of law keep such new technologies manageable and controllable?

Making these technologies public is a core concept in the answer to both questions – hence the title of this book, 'Making Surveillance Public'. This concept is first and foremost based on the idea that surveillance makes individuals' activities visible, but that its methods often remain invisible to the general public. Making surveillance public stands for revealing what is hidden and what is no longer seen as surveillance. It also relates to the societal role of surveillance, namely contributing to security, which can be seen as the ultimate public good. In this way, AI can be used to significantly improve efficiency in the prevention and detection of crime and antisocial behaviour and in developing security policy by local authorities and national government.

At the same time, AI applications affect fundamental values and their application should comply with underpinning principles as well as procedural values. On the one hand, public values are about legal principles relating to our collective and individual freedom such as the right to equal treatment and the privacy of citizens, while on the other, they stand for good implementation of procedural principles, including creating accountability and transparency around algorithms (WRR, 2011). All these different dimensions of making surveillance public intrinsically conceal a tension which in part logically arises from the fact that many AI applications have to be implemented out of sight and hidden from citizens, as in the case of automated searches of the dark web ('data crawling') by the police, for instance to detect child pornography or arms dealing. Complete openness is not always deliverable or even desirable

(due to privacy considerations), but more on instrumentality and legal protection later.

A sharp look at the public dimension of surveillance also raises questions as to the power relationships between public and private parties and the position of the private companies mentioned above – Amazon, Tesla and Google – in security provision. The fact that these parties are increasingly frequently and extensively involved in facilitating security provision, carrying out police-like tasks and working with large data sets and algorithms while being subject to far fewer regulations than the state or public-sector parties, is another aspect of making surveillance public. In this context, public values relate to issues such as an even playing field when it comes to security. Market power and data power can be a dangerous cocktail, especially if there is a substantial lack of legal clarity in issues such as ownership of data. Who owns the data people leave behind on Amazon and Tesla's digital platforms, for instance? Who is permitted to see this personal data and use it for other purposes? In short, what new regulatory issues are involved for the government, given its responsibility for security?

In all this I would like to distance myself from a line of thought about AI in which the presumed technical and economic advantages prevail and sociological aspects such as 'power', 'knowledge' and 'experiences' remain underexposed. It sometimes seems that the AI debate is confined to efficiency and efficacy – often stemming from the idea that technology itself is neutral. This technical and economic approach focuses on issues such as the speed with which very large volumes of data

can be collected or on efficiency arguments, where both work processes and crime detection are comprehensively improved by the use of AI applications. These, too, are public values and it is understandable that efficiency and efficacy are seen as important criteria for evaluation, but I argue that the reality of AI in practice generally contrasts with our expectations, not in terms of its enormous technological and economic potential in detecting crime, but in that these technologies must always be viewed in relation to the social environment they form a part of.

In short, there is no society without technology and there is no technology without society. This makes everything socio-technological and all oppositions between humans and technology or between the social and the technological unfounded – a simple argument that is still not well understood. It means that AI is also always a social practice, and that the experiences of individuals who come into contact with AI, from security professionals and consumers of luxury surveillance to citizens who are assessed as representing a high security risk, must be involved in academic research on the subject. Making surveillance public is then a matter of collecting the voices of all those affected by a surveillance issue, and in my opinion more attention should be paid to the manner in which each technology works as a template, whereby the knowledge of particular individuals such as data professionals can gain the upper hand and those of other individuals can be forgotten or viewed as worthless.

In order to investigate all this, I will approach 'making surveillance public' from different perspectives and I do so in the following steps. First of all, I focus on the phenomenon of data donation and its central question: why do citizens voluntarily give away their most personal data to companies? I then discuss the central place of surveillance in our society and key developments in this area. Based on the example of the Waze navigation app, I look into the connection between technological innovation and intensification of new power relationships, which I refer to as algorithmic psychopower. Within the broad palette of AI applications, I then focus on the phenomenon of big data policing. I then discuss which films, books and series offer thought-provoking material on AI and digital surveillance. The next central issue I approach is how AI applications can be kept manageable and controllable, identifying key points and stumbling blocks. This is followed by the issue of what knowledge we need to focus on, where I propose making experiences of AI a component of good care for technology. I conclude with the issue of how criminological research can contribute to further thinking through and developing AI's role in security.

Interlude I. Data Donation

On my screen I read a newspaper report that states that Dutch hospitals save patient data in the cloud using the American Amazon Web Services. The same article claims that the patients themselves are unaware of this, and that if the National Security Agency or another intelligence service wants to inspect their medical records, they're powerless to prevent it. The report reminds me of the expression 'data is the new oil' – a saying that's trotted out so often that it has become a cliché and can't really be used in serious discourse anymore, but which, like many clichés, contains a grain of truth. Whether we're talking about hospitals, government or private companies, data fuels their work and ensures that AI systems function. It determines whether a diagnosis is correct or who is right, but also what actions are necessary and which products and services should be improved. Except that data alone is not enough. Data has to come from somewhere, and we often give it away without thinking about what will happen to it afterwards. But why do we voluntarily give away our most personal data to other parties? That's what interests me in the newspaper report.

Scientific research has been conducted into which factors play a role in sharing our personal data with other parties. A number of clear and well-constructed rationales have come out of this, which can be broadly distinguished on the basis of the domain in which data sharing takes place. For instance, citizens are constantly sharing their data with the government. This data is used by the government for policy forming processes, to better understand needs and preferences of citizens or to design and offer products or services. Prosocial behaviour and community-focused motives play an important role here. At the same time, people are also led by self-interest, as shown by an increase of citizen support for sharing their data for the sake of government policy if they expect a personal benefit from it (Trein & Varone, 2023).

Data sharing also plays a key role historically in the medical world, where it is completely interwoven with medical research and clinical practice. You could call donating blood, organs or tissue a forerunner of data sharing – in the context of health research or to help others, for instance in the case of a family member offering a kidney for transplant. In the decision to donate blood, the interests of others tend to come first. The common good is also central to consent for use of our personal data, including what we eat and drink, how long we sleep and how much we exercise. In addition to this, a recent study involving 1300 participants identified three distinct reasons that influence people in donating sensitive data for medical research. An opportunity to achieve self-benefit and a sense of social duty turn out to be the most important motives, and empirical research also shows that people are more inclined to

donate their data when they know what it will be used for (Skatova & Goulding, 2019).

Although more and more research is being done into the motives for sharing personal data with hospitals and the government, we know little about what drives people to do so with large private companies through internet sites or apps. This needs to be examined more closely, not least because it relates to data that people prefer not to share. Take Tesla's electric cars and the way data sharing leads to the tech company knowing everything about the people inside. With the owner's permission, the car brand gains insight into details such as the driver's temperature preferences and favourite destinations. In order to make this possible, driving behaviour is recorded by inbuilt cameras, the positions of the steering wheel and external mirrors are registered, and the system notes how much the driver uses the accelerator, how they take corners and their average brake usage. On top of that, Sentry Mode uses the cameras to record suspicious activities outside the car when it's parked and locked. As a result, the driver's everyday activity and everything outside the car are continuously watched by Tesla, which stores all the data in a unique driver profile.

The Mozilla Foundation, an organisation that works to map out the role of the internet in people's lives, has listed what personal data the car manufacturers have access to.[1] Research into 25 car brands reveals the excessive data collection by these companies. Not only is far more data collected than is strictly necessary – from your medical and genetic information to your sex life (Nissan) – it also turns out that 84% of the

car companies in the study share customers' data with service providers, data brokers and investigation agencies. Nineteen manufacturers also pass on data to other parties, including insurance companies. Of all the companies studied, Tesla failed all of the reviews that looked at security, data control and AI, making them by far the worst of all cars studied. In reference to Foucault, the Tesla can best be described as a digital panopticar.

In her book *The Age of Surveillance Capitalism*, Shoshana Zuboff (2019) pointed to the benefits reaped by a handful of large tech companies from the data we give them. A possible explanation for the ease with which this happens is undoubtedly the quick and simple means of giving online consent to share our data – a mere tick of a box is sufficient, which means that no one reads the conditions of use that appear on the screen. It probably also relates to the fact that we never stop to think about public values such as privacy and data protection. In many cases, people are ignorant of their rights when it comes to data sharing, and we don't really know what happens to the data we share with tech companies. All this means that data sharing is hardly ever seen as a problem, which makes us incapable of assessing in which way giving away data differs from donating blood or a part of one's liver.

However, history teaches us that there are sociological lessons that can be applied to the phenomenon of data sharing. What private companies advertise and attempt to sell through their platforms is in fact the promise of ever better products. They need our data for this, turning people into walking cash dispensers – with the side note that we're not passive objects but

actively participating. In this respect, the idea of willingly giving up your personal data in exchange for something valuable in many ways resembles what the French anthropologist Marcel Mauss in his essay by the same title termed 'the gift' (2002 [1923-1924]). The gift is the cement of society, a social phenomenon through which an entire society expresses itself. We know from anthropological literature that asymmetric power relationships are an important aspect of gift giving (Lévi-Strauss, 1969 [1949]); Gouldner, 1960). In other words, if you understand the long-standing system of giving and receiving, then you hold the keys to digital modernity. Of course, our time bears little resemblance to the gift economy as it existed in Polynesia, Melanesia, and the American Northwest, but that doesn't exclude the possibility of personal data being the modern equivalent of the gift. The difference is that in exchange we now receive free products, better services, exclusive content or financial advantages, such as reduced premiums on insurance for the Tesla.

Altogether there is something paradoxical and vicious about data donation. The underlying motives will reflect more self-interest than gifts in a personal context, while at the same time, more and more judicial initiatives are being developed to give citizens more say over their data and the conditions in which it is shared with other parties. This leads to the paradoxical situation that while the system of the gift is becoming increasingly constrained and legally restricted, history has shown that it is the voluntary transfer of socially valuable objects which actually makes our society possible.

2 Digital Surveillance

2.1 Introduction

Before going deeper into big data policing, it's worth considering the issue of surveillance in a more general sense. The question of AI in the detection and prevention of crime and anti-social behaviour cannot be answered without greater focus on surveillance in society and why digital technologies have taken over control in all aspects of our lives. A key factor here is that surveillance is not an isolated or independent development. It's embedded in a series of longer-running developments that are technological, economic and political in nature. Such broad developments contribute to a situation in which many of the characteristics of traditional surveillance, as I previously described it, are no longer self-evident. In order to emphasise the difference with traditional surveillance, Gary Marx speaks of 'new surveillance', which he describes as 'the scrutiny of individuals, groups, and contexts through the use of technical means to extract or create information' (2002; 2016: 20).

Binary classifications such as old/new never really do justice to the nature of surveillance in the long term, but what I'm interested in now is giving a more precise interpretation of the question of what is *new* about many current forms of surveillance. I distinguish eight developments. This is not an exhaustive list and each requires nuance, but these issues are regularly mentioned in the literature and have led to a substantial expansion in both the scope and the depth of surveillance. They range from mass data collection in domains such as education, mobility and healthcare to radical invasion of the private lives of citizens using surveillance technologies which are no longer recognised as such because they have become part of daily life, including smart doorbells, toothbrushes, TVs, fridges and washing machines as well as thermostats that can make decisions for themselves. My claim is that all this has led to a society dominated by surveillance. Surveillance organises and orientates society, with everyone participating to a greater or lesser extent.

2.2 From digitalisation to commodification

In order to better understand how new forms of surveillance are infiltrating faster, broader and deeper into society and into the daily lives of citizens, in this section I discuss various developments that have contributed to surveillance playing such a major role, with all the characteristics common to new forms of surveillance.

a. Digitalisation and AI

Digitalisation is a collective term for a large group of new technologies that have been used in ever more domains over the last few decades. Rapid developments in digitalisation make it impossible to give an exhaustive list, but this might include applications that are now used within the broad area of AI, such as biometric recognition, predictions of risk and success, algorithmic decision-making, automatic translation, recommendation systems, etc. These applications have found their way into many sectors of society, such as education, financial services, transport, healthcare and law enforcement. They effectively form the engine of our society by maintaining its underlying organisation, which makes digitalisation and AI – just like our water supply, road network or electricity grid – so important that they exhibit all the characteristics of new infrastructure. In relation to AI, the term 'system technology' is used here, an invention with a systemic effect for the whole of society, as electricity was in the nineteenth century and the combustion engine in the twentieth (WRR, 2023).

We live in a digital age in which ever more aspects of our lives play out online and the distinction between physical and digital is increasingly blurred. In this situation, digitalisation and AI can easily be connected with the latest developments in crime – put simply, society is becoming digitalised and so is crime.[1] Examples include traditional crimes such as money laundering, child pornography and drug dealing which are now also committed over the internet, e-mail or an app. New forms of crime have further arisen through digitalisation, such

as hacks, ransomware, doxing and spreading computer viruses. There are fears that criminals and terrorists can also deploy AI applications, including deep fakes, voice cloning and the use of driverless vehicles as weapons of terror ('malicious AI').[2] Digitalisation and AI also have consequences for the scope of crime. From the latest figures it may appear that reported crime in many Western countries has fallen by more than a quarter since 2002, but that drop does not apply to cybercrime. Over the last few years in particular, there has been a substantial rise in victims of cybercrime, which has undergone the opposite trend and is expected to continue to rise over the next few years.[3]

Criminology and security policies pay a great deal of attention to cybercrime and cyber security. More and more people are falling victim to these crimes and the impact on society is substantial. There is far less attention for the fact that digitalisation and AI have also turbo-charged the detection and enforcement of crime and even radically changed sanctions and the execution of sentences. The question here is whether the current legal frameworks and institutional supervision are sufficient to maintain control of legal and ethical issues such as excluding dirty data while ensuring public values such as non-discrimination. This becomes clear when you take a closer look at digitalisation and AI, as in the case of the OxRec algorithm which is used by the Dutch Probation Service to advise judges on a suspect's risk of recidivism. This involves estimating the chance of recidivism, which raises questions as to the potential for unequal treatment based on race, social class and other social inequalities (Maas, Legters & Fazel, 2020; Van Dijck, 2020).[4] I will return to these issues in the following chapters.

b. Datafication

With digitalisation, the volume, variety and velocity of data increase exponentially. This leads to the phenomenon of datafication, the conversion of actions into data, where the following aspects can be distinguished: the scope of the data, its nature and analysis, as well as its scope of application (Mayer-Schönberger & Cukier, 2013; WRR, 2015: 24-26).[5] As a result of digitalisation, more data-producing items are entering our environment and there is more data available that say something about our lives. The plethora of appliances connected to the internet (the Internet of Things) and product innovations such as consumer databases, data warehouses and computer clouds is making the mountain of digital data ever larger. New AI capabilities for analysing these data collections have led to a growth in the number of surveillance applications in different domains. Data can be the product of targeted collection or automated processes, or it can be provided by individuals voluntarily (Kitchin, 2014a). A relevant point here is that in principle anything can be data, however small, trivial or insignificant, from work processes and sport to the actions of individuals in everyday life.

Digitalisation and datafication constantly reinforce one another and offer new opportunities for surveillance, referred to by Roger Clarke as 'dataveillance': 'the systematic investigation or monitoring of the actions or communications of one or more persons' (1988: 499). This leads to a situation in which surveillance often takes place outside the control and sight of individuals or groups and without their knowledge or consent.

Dataveillance changes the distinction between individual and mass surveillance, making the difference ever smaller. Dataveillance makes use of profiles to support decision-making processes and treat individuals differently if they are allocated to different profiles. This is known as 'social sorting', whereby 'existing social differences and divisions are reproduced and reinforced, extended and mutated' (Lyon, 2001: 151, see also: Gandy, 1993). In this regard, Kevin Haggerty and Richard Ericson (2000) speak of the 'data double' and point out that different parties split individuals into pieces of relevant information that are then used and combined in a specific context, in the framework of risk profiles (combatting terrorism) or for commercial purposes (consumer profiles), for instance.[6] You could also say that we are transforming from collections of cells to collections of data; a process that leads to the addition of a digital identity to our physical existence. The consequence is that the 'in-dividual' – an 'in-divisible entity' – is decentred to a 'dividual', a substance that never ceases to split into ever smaller units that can be deployed by diverse parties for diverse purposes. Consequently, the paradigm of the autonomous and sovereign subject no longer serves as a heuristic point of departure. We are entities with many roles, represented in various datasets (Koopman, 2019). 'Digitalisation is dividualisation', the philosopher Miriam Rasch writes in *Frictie* (2020: 86).

c. *Algorithmisation*

Now that digitalisation and datafication have come to be so central to the way in which society organises itself, algorithms

ensure that data collection (*input*) leads via processing (*throughput*) to a conclusion (*output*). An algorithm is basically a series of instructions that leads to a calculation of an outcome for a problem. It can be compared with a recipe: by following a number of set steps, you prepare a dish that you can serve. That one word, algorithm, however, covers many different types. There are logical rules ('rule-based algorithms') which operate on the basis of formulas of the type 'if A, then B'. In more complex forms, there are algorithms which attempt to achieve a particular aim by themselves without being given explicit instructions. Complex reasoning involves connectionism, including variants such as machine learning and deep learning algorithms, which in turn can be subdivided into different forms ('supervised', 'semi-supervised' or 'unsupervised'). In the example of the recipe, the algorithm then prepares a dish without knowing all the ingredients in advance.

The rapid growth in the use of algorithms, ranging from applications in the education and care sectors to uses in government, has drawn increasing attention to the risks of AI. An algorithm is not an objective calculator without character or direction. It is set up by developers, analysts and policy makers, and this means that it is politically and culturally sensitive. Many unforeseen effects can therefore arise, with the potential, depending on the context and nature of the application, for a substantial impact. Predictive policing, for example, raises sociotechnological risks such as discrimination against minorities, increased inequality, stigmatisation and overpolicing as a result of technical bias and feedback loops (e.g., O'Neil, 2016; Ferguson, 2017; Benjamin, 2019). There are also constitutional

concerns in this context, varying from the importance of clean data, function creep in the form of reuse of data for purposes different from those originally established, fishing expeditions and spurious correlations, where causal connections are wrongfully made, right through to violation of the presumption of innocence and bureaucratisation (the 'digital cage') (e.g., Kraft, 2018; Peeters & Schuilenburg, 2018; Richardson, Schultz & Crawford, 2019; Das & Schuilenburg, 2020).

In this light, new legal issues arise, such as the demand for accountability – in criminal or civil law – of the people who have designed the algorithm. Frank Pasquale (2015) also points to the so-called black box scenario, the fact that algorithmic decision-making is inaccessible to outsiders and thus cannot be checked, and can even no longer be understood or explained by the users themselves. Finally, in algorithmisation there is the problem that if the government in collecting and processing data leans entirely on private parties, relinquishing data, expertise and intellectual property rights, which poses a threat to disclosure and the ability to explain the datasets and algorithms used (Zuboff, 2019).

d. Multisensory

A fourth development I would like to mention here is that surveillance no longer depends on the naked eye – the traditional watching and being watched, which recurs in concepts such as the panoptic gaze and the principle of constant visibility – technological developments have also made hearing,

smell and taste important sources of information. Using the terms of the Canadian media philosopher Marshall McLuhan, you might say that surveillance has become an extension of all human senses. An interesting aspect of this is that of all sensory organs the nose is the only one that can 'look' back in time. While scent works retrospectively, sight and hearing provide real-time analysis, carried out by digital sensors which explore the surroundings for strange noises or movements and take action if necessary, such as giving a warning by sounding an alarm. For instance, there are streetlights in high-burglary-risk areas which, aided by complex algorithms, recognise suspicious sounds such as breaking glass, bangs and shouting, in order to detect an attempted break-in. These streetlights can also analyse the gait of passers-by for signs that a burglar is exploring the neighbourhood or that pickpockets are operating there.

Mark Andrejevic and Mark Burdon (2015) talk of a 'sensor society' and point to the enormous growth in sensory technology and the volume of sensory data that is generated by this. The potential of sensors has been enormously expanded in recent years. Sensors have become smaller, more mobile and cheaper and can be worn on the body (bodycams, watches or glasses) or attached to objects such as vehicles, security cameras, parking meters, waste containers and entry gates to airports or in football stadiums. The term 'smart' is often used for these applications, referring to sensors with an internet connection that collect data with the aim of improving quality of life. Think of smart sensors in waste containers used to improve collection routes for rubbish trucks and make them quicker to detect antisocial behaviour such as dumping waste. The processing of

data by smart sensor surveillance can be visualised in terms of a 'cybernetic control loop' or 'digital control loop' that consists of collection, analysis and application, constantly optimising the intervention by measuring efficacy and adjusting the intervention where necessary on the basis of the results. These steps largely coincide with the steps the police distinguish for data-driven detection: 'collect, store, analyse and engage' (Van de Sandt et al., 2021).

e. Softening

An important aspect related to the developments of digitalisation and datafication mentioned above, is that – compared with traditional surveillance – new surveillance methods have become less visible and intrusive. This represents a 'softening' or 'soft power' in surveillance. In *Windows into the Soul*, Gary Marx (2016: ch. 5) gives various examples of this, from urine and DNA tests to scanning equipment at airports that makes it possible to search people without requiring physical contact. The soft forms of information acquisition contrast with 'hard', traditional forms, such as police interrogations, traffic stops or house searches, where it should be noted that the opposition between 'soft' and 'hard' has nothing to do with the extent of infringement on fundamental human rights in someone's personal life. 'So soft, it's hard'; by which I mean to say that the least visible forms of surveillance can have the most radical consequences for citizens. Recent examples include the Dutch *Systeem Risico Indicatie* (SyRI), now banned in the Netherlands, which was set up to detect benefit fraud in deprived areas, and

the use of algorithms by the Dutch Tax and Customs Authority in the childcare benefits scandal ('Toeslagenaffaire') that came to light in 2018.[7] In the latter case, thousands of families claiming tax allowances to pay for childcare were falsely accused of social benefits fraud if they made minor errors in their paperwork, such as failing to submit supporting documents on time.

The softening of surveillance technology is also reflected in language. Digital modernity is characterised by light-hearted, casual and cute concepts such as 'cookies', 'Wi-Fi', 'airdrop', 'airplay' and 'the cloud'. A contributing factor in the softening of surveillance is the fact that the technology can be simply built into everyday products, such as cameras in smartphones or, in the case of RFID chips the size of a grain of sand, in e-bikes, laptops and watches. This makes surveillance largely invisible and intangible – and in many cases even intimate. There is less consideration of the fact that in all this the embedding of 'computing machinery, more or less invisibly, in the environments of everyday life' (Lyon, 2018: 51) has dehumanised surveillance. The minimal visibility of digital and algorithmic surveillance represents a break with the recognisability of security professionals in uniforms, as in the case of visible monitoring by private security personnel in shopping centres, police officers in the street or customs officials at airports ('visible policing'). The dehumanisation of surveillance can eventually lead to a complete lack of meaningful human checks or points of contact, leaving human authority completely out of the loop, an issue relevant to automatic and autonomous weapons systems such as unmanned aircraft, swarms of drones and killer robots.[8]

f. Everybody's doing it

Surveillance technology is changing rapidly, as are its users. Anyone who takes surveillance to mean the sovereign power of government runs the risk of missing many aspects of the subject. Surveillance applications to make society safe are no longer the preserve of the police and other specialised government organisations. Surveillance also takes place 'beyond' the police, in the form of commercial companies, and 'below' the police, by citizens effectively engaging in 'do-it-yourself surveillance' or 'wikiveillance'. With smartphones, almost all citizens have cameras on them 24 hours a day with which they can film, record, or take photos of others. The footage can be used for personal purposes, but also serve public aims, for instance as evidence in the prosecution or detection of crime by the police. In short, anyone who thinks surveillance is only about a world of 'spies, police and the state' (Marx, 2016: xv) has been deceived.

I'll go into more detail on the blurring of the boundaries between public and private surveillance later, but for now it's important to emphasise that this development is not entirely the same as the democratisation of surveillance. Without wishing to diminish related notions such as 'synoptic surveillance' (Mathiesen, 1997), whereby the many observe the few, and 'sousveillance', surveillance from below (including variants such as 'co-veillance'), whereby citizens themselves are active overseers (Mann, Nolan & Wellman, 2003), it could be argued that such notions imply that differences in power and knowledge between government and other parties can be re-

duced.[9] Thus sousveillance is supposed to reverse the power relationship between government and individuals and restore 'a traditional balance that the institutionalization of Bentham's Panopticon itself disrupted' (Mann, Nolan & Wellman, 2003: 347). But this does not apply across the board or to all forms of new surveillance. In the current surveillance landscape, some groups remain more powerful than others. The powerful are now primarily what Shoshana Zuboff (2019) has termed 'surveillance capitalists' – private tech companies whose revenue model is based on collecting as much behavioural data as possible and selling it to third parties so that products and services can be targeted at the individual.

g. Commodification

Another recent development is the fact that the data collected by surveillance has acquired value and can be traded. One of the first studies on this is Oscar Gandy's book on consumer surveillance, *The Panoptic Sort* (1993), in which he describes how personal information is gaining economic value in business. Where traditional capitalism converts material resources and labour into tradable goods and products, in surveillance capitalism the revenue model shifts to data that had little or no independent value in the 'old' economy, including factual data and genetic information. Online conversations on Facebook, for example, have economic value and can be sold to companies. Even search terms containing spelling mistakes or the use of exclamation marks on Google generate valuable information and are collected by companies. The data produced by platform

users – consciously or unconsciously, actively or passively – is effectively a form of free labour or immaterial labour. It's not seen as work, but still creates value because the result can be used or sold to other parties (Lazzarato, 1996; Arvidsson, 2006; 2010; Kienscherf, 2022). Data has become merchandise and on this point Zuboff (2019) speaks of a 'behavioural surplus' – the use of digital traces people leave behind when they are active on the internet to improve products or services or tune adverts and offers to individual preferences. 'Silent theft' would in fact be a better term.

Surveillance capitalists such as Facebook, Amazon and Google play an important role in the commodification of information – the online transformation of personal data into tradable products and services that have economic value and are subject to property rights. This happens on digital platforms which provide the technological, economic and socio-cultural infrastructure 'to monopolise, extract, analyse, and use the increasingly large amounts of data that were recorded' (Srnicek, 2017: 43). There are few domains that remain untouched by the rise of digital platforms.[10] Whether we're talking about the neighbourhood (Nextdoor), hotel chains (Airbnb), transport (Uber) or education (Coursera), almost all walks of life have seen a partial move of social and services trade to a digital environment. In the literature on digital platforms, most attention is focused on commercial purposes, but police activity also increasingly takes place within a closed platform world. For instance, the internet in general and social media platforms such as TikTok, X and Telegram in particular are a (relatively new) source of data collection by the police. These are used

in the detection of crime ('internet investigation') or gathering online data for the sake of intelligence, known as 'open-source intelligence' (OSINT). OSINT involves features such as identifying trends or threats in society and monitoring individuals and groups for issues such as social unrest.[11] The police also use their own digital platforms. Besides reporting crime digitally, you can contact web care teams and talk to a virtual agent, an AI chatbot that 'speaks' with people who want to report a crime. Finally, the police themselves have developed digital platforms in order to work with other parties on detection, as in the case of the Samen Zoeken ('Search Together') app the Dutch police are working on, which is intended to better coordinate police searches for missing persons with the help of citizens. Police work is thus shifting ever further towards 'platform policing'.[12]

h. Normalisation

The final recent development I would like to discuss is the integration of surveillance into our routine activities and lifestyle. David Lyon writes: 'Our whole way of life in the contemporary world is suffused with surveillance' (2007: 25). Examples range from luxury surveillance products such as the Apple Watch and the Fitbit, which are chock-full of sensors, including an electronic heart rate sensor and temperature sensor with which you can monitor your health and sports performance, to products on the work floor (Levy, 2022), in class (Whitman, 2020), around the house (Maalsen & Sadowski, 2019; Sadowski, Strengers & Kennedy, 2021), in the car (Eski & Schuilenburg,

2022) and even rigging up entire smart cities (Kitchin, 2014b; Schuilenburg & Peeters, 2018; Pali & Schuilenburg, 2020). We don't notice we're being monitored because it's become an everyday thing, part of routine actions; it's as normal as getting dressed before going to work or the fact that a day lasts 24 hours. The emphasis on surveillance and innovation is so great that there's even a toilet on the market that recognises users by their backsides and measures faeces and urine for values such as excessive protein, unhealthy substances or other peculiarities. In this form of 'facial recognition', the anus is a kind of fingerprint and people's health data are directly recorded in the electronic patient file.[13] Mark Andrejevic (2012) speaks of 'ubiquitous surveillance', pointing to a society in which it is becoming ever more difficult go unmonitored because almost everything contains a digital component generating data for use in a surveillance framework. You might say that surveillance has been domesticated and tamed – and thus normalised.

From the Ray-Ban Stories glasses with inbuilt cameras and microphones to record videos, to the voice-operated iRobot vacuum cleaner with smart mapping technology, in the world of big data nothing is too small to be used for surveillance. An important reason behind this is that increasingly advanced technologies make it possible to exploit even the very smallest data collections and relate them to one another for surveillance purposes. The datasets used now are also much smaller than the datasets of the era when the term 'big data' was introduced (Kitchin & McArdle, 2016).[14] In other words, big data is a gradual concept and subject to inflation. Nowadays, it primar-

ily comprises a great variety of types of data and not so much large volumes.

In this context it's worth mentioning 'little tech', surveillance products at work or at home that constantly collect data, from Apple AirTags that you attach to objects such as key rings to monitor their location, to the voice-operated assistant Google Nest Hub with an inbuilt camera to keep an eye on things while you're out and about. The way data is collected and recorded by such everyday devices infringes on public values such as privacy and transparency, yet so far it has not received the same kind of attention as cases such as the data-analysis company Cambridge Analytica, which abused the personal data of millions of American Facebook users for tailored political influence campaigns. That's not surprising and very understandable, but the consequences of the algorithmic colonisation of the private domain are hard to ignore. It would only be a slight exaggeration to describe the situation as follows: forget Big Tech, the real threat is Little Tech.

2.3 Algorithmic governance

When you think about it, surveillance has always been around. It's nothing new. In many respects, surveillance is a natural part of human existence, at play in almost everything we do – it would raise eyebrows if there were no checks at airports and swimming pools. The recent development of digitalisation, however, has meant that surveillance has grown to unprecedented proportions, bringing with it large-scale data collection

across society carried out by a motley crew of public and private parties. This has created a new infrastructure cutting straight across all domains, from security and mobility to education, which has become vital to society. In this respect, surveillance is reminiscent of a parable told by the American writer David Foster Wallace in 2005 to a group of graduates of Kenyon College, about two young fish who come across an older fish swimming in the opposite direction. 'Morning, boys. How's the water?' the old fish asks. The two young fish swim on and when the old fish is out of sight, they say to each other, 'What the hell is water?'

In a world plastered over with surveillance, many parties employ a technical-economic perspective to legitimise the use of AI in their work processes. This is a depoliticised approach in which big data and algorithms are taken as a means of achieving a desired aim more efficiently (faster cheaper, and with less effort). This perspective follows from a goal-oriented rationale, based on factors such as cost effectiveness, calculability and predictability.[15] Costs and benefits are weighed up and scarce resources can be deployed more economically to optimise the outcome. To put it philosophically, truth is reduced here to provability, which in turn is reduced to calculability.

This calculating approach dates back to the work of the jurist and sociologist Max Weber (2006 [1921/1922]), in which he draws an opposition between goal-oriented rational action ('zweckrational') and action based on values ('wertrational'). According to Weber, goal-oriented rational action is gaining dominance in our society and forms the engine of the bureau-

cratisation of state administration. To Weber, this conjures up the image of bureaucracy as an 'iron cage' ('stahlhartes Gehäuse') in which thinking about public values is repressed in favour of self-perpetuating formal regulations and procedures. He speaks of 'the cold skeleton hands of rational orders' (1988: 560) and points out that there is no space in a bureaucratic administration for personal or emotional elements.[16] From his view of bureaucracy it follows that people are compelled to follow regulations and procedures formulated by others, which can get in the way of the values an organisation should strive for (Schreurs, 2003; De Jong, 2016). In the police force, for example, it is never exclusively about measures of efficiency and efficacy; public values such as fairness and equal treatment of citizens are also important.

Along the same line as Weber, in *Seeing Like a State* (1998), subtitled *How Certain Schemes to Improve the Human Condition Have Failed*, James Scott points to the fact that increasing rationalisation processes in organising society lead to an erosion of certain forms of knowledge. He relates this to local knowledge and the skills of particular groups of people. In doing so, Scott hits a sore spot that in goal-oriented rational action the knowledge of particular individuals can be excluded, because a form of human knowledge is no longer viewed as useful, or because not all citizens count equally or have the right to representation in the predominant perspective in a society. Scott uses the ancient Greek notion of *mētis*, which refers to a range of practical experiences and skills that cannot be completely standardised, as in the case of a farmer who knows the right moment to sow or harvest. This ungeneralisable knowledge

which takes into account local complexity is seen in opposition to *technê* (from which words such as 'technology' are derived). *Technê* is universal, abstracted knowledge that offers control over situations and which, in Scott's words, is characterised by 'impersonal, often quantitative precision and a concern with explanation and verification' (1998: 320). I return to this in the Interlude on AI experiences.

In today's world, bureaucratic forms of control seem to be making way for algorithmic governance. This phenomenon is also known as 'algocracy', a term coined by Aneesh Aneesh (2006; 2009), in which the processing power of algorithms has come to play a central role in the functioning of government, and in which the government is highly dependent on algorithms in carrying out its tasks.[17] Aneesh also starts out from a Weberian notion of bureaucracy and shows how algorithms add a new dimension to existing forms of digital administration ('e-government'). In this way the iron cage of traditional bureaucracy is augmented or even replaced by a 'digital cage' (Peeters & Widlak, 2018) – or rather, an 'algorithmic cage'. As in traditional bureaucracy, with its formal rules and procedures, algorithms focus on efficient outcomes based on agreed criteria. The problem is that legitimacy shifts in an algocracy from written rules to invisible algorithms, and officials often don't know what rules these algorithms are following. 'Authority is increasingly expressed algorithmically,' Frank Pasquale (2015: 8) observes. Along the same lines, Scott Lash argues that power 'is increasingly *in* the algorithm' (2007: 71) and David Beer writes that power works '*through* the algorithm' (2009), which raises new questions as to what institutional

mechanisms need developing to guarantee that the use of algorithms will not lead to an erosion of government legitimacy (Busuioc, 2021; Meijer, Grimmelikhuijsen & Bovens, 2021).

However valuable the descriptions above may be when it comes to issues such as algocracy and calls in public administration studies for greater public accountability in the use of algorithms by government organisations, they fall short when it comes to a substantive solution for making surveillance public. One reason for this is that evaluation of the use of AI applications and the dilemmas and potential risks they raise can never be generic; it always requires examination of the practice in which the applications are deployed. In other words, there are always individual considerations in surveillance. For one thing, the purpose of a specific AI application makes a considerable difference. The dilemmas and risks will be different, for instance, when it comes to a tool for digitalising routine tasks in education as compared with predicting burglaries based on police information, supplemented with information from public datasets, as in the case of predictive policing. After all, applications in the context of operational management are of a different order from the deployment of AI to improve detection of crime.

It also makes a considerable difference what type of algorithm is used in an AI application. One algorithm is not the same as another. The risks to citizens, such as ethnic profiling and discrimination against minorities, turn out to be far greater when an algorithm is given free rein, as in the case of machine-learning, than when it comes to a simple decision

tree ('rule-based') with a limited number of variables. A third side note is that it is also important to consider the domain in which AI is used. For parties with a function in criminal law, such as the police or judicial authorities, the use of AI will raise different ethical and legal challenges than for other public or private organisations. For instance, in tracking crime the police are allowed to infringe fundamental human rights, such as the right to privacy, but this comes with strict requirements and is bound by the necessary safeguards.

In short, the problem is that the current academic and public discourse on AI itself still exhibits many characteristics of a black box, and in order to open that box we will first have to consider the aim and practical context of a particular application. In chapter 3, I take a closer look at the phenomenon of big data policing. But first I explore a somewhat personally tinted occurrence to illustrate how digital surveillance is always an expression of power relationships for governing life.

Interlude II. Algorithmic Psychopower

Before we get into the Tesla, I enter the street and house number of the Italian restaurant we're going to this evening into the navigation app Waze. The journey is 23.6 kilometres and according to the app, the journey should go smoothly. Various routes are coloured green, which means there's no heavy traffic. When I select the shortest, quickest and most obvious route to the restaurant, a message comes up on the screen suggesting I take the longest route. It's safer not to drive through a particular neighbourhood, which according to the route planner is a 'high-risk area' with very high crime rates, and Waze recommends a way to avoid it. The travel time difference is eleven minutes and I decide to take the slowest route to the restaurant instead of the fastest.

Waze is a free navigation app for Android and iPhone, developed in Israel and bought by Google in 2013. It offers 'community-based traffic' information, which entails the use of data from all Waze users to find the optimal route. It gives warnings in time for speed cameras, police, road works and

accidents reported by other users. But Waze also warns users via the 'Avoid Dangerous Neighbourhoods' function when you're about to drive into an unsafe neighbourhood and recommends routes that avoid these areas, even if driving through them would be faster.

Waze is the latest navigation app to use AI and algorithms to gently nudge human behaviour in a particular direction. Initially the 'Avoid Dangerous Neighbourhoods' function was only available in Israel and Brazil, but it has now been rolled out to more countries (Leszczynski, 2016; Carraro, 2021). Route planners with a comparable feature include SketchFactor, RedZone and Ghetto Tracker, whose name was later changed to Good Part of Town. Ted Farnsworth, founder of RedZone, says, 'We have designed RedZone Maps to show real-time crime data through its social listening, big data and artificial intelligence capabilities in a navigation map format.' The apps use crime figures from police forces and customer reviews of neighbourhoods, supplementing them with up-to-date user reports on crime and antisocial behaviour. A 'high-risk area' is coloured red and the navigation system's gender-neutral voice announces that you're approaching an 'area with risk of crime'. I use the term 'algorithmic psychopower' for these psychological stimuli which automatically influence and emotively guide users. The digital tools with which this form of power is deployed are hypernudges.

Michel Foucault wrote a great deal about power, distinguishing different types, with disciplinary power being the most famous form and biopolitics the most recent. According to Foucault,

the citizen is not a rationally operating 'homo legalis', but a category of the population to be disciplined and cared for. This is achieved on the one hand through tools such as drills and examinations in barracks, schools, factories and prisons, where people are made into obedient subjects who can be effectively deployed. Foucault calls this the 'anatomo-politics' of the human body (1976: 183; 2004: 243) and in his books *Surveiller et punir* (1975) and *La volonté de savoir* (1976) he constantly makes connections between physical bodies, power, knowledge and concrete spaces that draw a sharp boundary between internal and external. On the other hand, this effect is achieved through the control of the entire population with regulatory procedures to make life as a whole more prosperous, healthier and safer. Foucault (1976; 2008) speaks in this context of the biopolitics of the population, involving resources such as vaccination and improvements in hygiene. In practice this allows a growing government to assume responsibility for the living conditions of all citizens and the biological processes of their bodies.

Foucault's view has limited use in gaining a good understanding of algorithmic psychopower. In my opinion it falls short both when it comes to the digital turn in surveillance and in the ways in which psychological stimuli are given to steer the behaviour of individuals and groups in a desired direction. The limitations of Foucault's power thinking are all the clearer when placed alongside the views of the French philosopher of technology, Bernard Stiegler. Like Foucault, Stiegler is interested in technology as an effect of the exercise of power, but he places serious question marks around Foucault's emphasis

on discipline of the body and regulation of biological life by government. Stiegler's work is not simple to summarise and can only be represented schematically here, but in his view, a shift has taken place from biopolitics to what he calls 'psychopolitics' (*psychopolitique*) (2010).[1] He states that in today's world, a battle for the mind is raging in the media and he points to 'the radio (1920), television (1950) and digital technologies (1990), spreading all over the planet through various forms of networks, and resulting in a constant industrial canalization of attention' (2006). Stiegler believes that new media, even more than its traditional counterpart, is constantly attempting to capture our attention and desires and to lead in the direction of more consumption. An example would be the personalised advertisements on the internet which reduce existence to the level of direct satisfaction of needs. Referring to the work of Gilles Deleuze, he writes, 'A control society does not only consist in the installation, throughout society, of social control, but rather penetrates into consciousness … and thus reinstates corporate control' (2011: 82).

In the case of algorithmic psychopower, we see something comparable to what Stiegler sketches in broad brushstrokes, in the transition from biopolitics to a society of consumers. The key point of intervention for psychopower is not the body and life, but 'the soul' or the human 'mind' (psyche) of citizens.[2] In other words, while we still undergo discipline, it is now based on AI technologies that affect our consciousness and our desires, both on the level of accumulation (immaterial labour) and intervention (control and manipulation). The latter is achieved by giving people psychological stimuli at decisive moments,

steering them unobtrusively but very powerfully in the desired direction.

This is known in the literature as 'nudging'. Nudges push citizens gently in the right direction without restricting their freedom of choice (Thaler & Sunstein, 2008; Sunstein, 2014). Classic examples are the fly sticker in toilets to get men to aim at the middle of the toilet bowl rather than the edge, healthy products placed at eye level in the supermarket, and the use of smaller plates and glasses in canteens. But algorithmic psychopower differs from traditional nudges in at least two important ways. Unlike these analogue nudges, algorithmic behaviour manipulation can be constantly automatically adjusted to changing circumstances. It's also possible to personalise and tailor it, so that only the intended recipient is nudged. When nudging is combined with big data and algorithms and has a specific point of intervention rather than a generic one, we can speak of e-nudging, big nudging or hypernudging (Yeung, 2017).

In the case of the navigation app Waze, the option of an independent decision remains (in other words, you can take the shortest, fastest route), but I am effectively tempted to make a different choice. All kinds of things happen inside me from the moment that Waze suggests a different route to the Italian restaurant. The colour red on my screen sets off powerful emotions, conjuring up connotations of danger. In a philosophical sense you might say that the seduction of the object is stronger than the desire of the subject to take the shortest route.

But this example of algorithmic psychopower also shows how AI lays down invisible barbed wire across an urban area. You could even say that geosurveillance generates a form of data violence – less visible than verbal or physical violence, but no less violent. This follows from the fact that psychopower is part of political and economic structures and reflects a long history of exclusion mechanisms, based on racist images of ethnicity and social class. The name 'Ghetto Tracker' says it all. In her book *Race After Technology*, Ruha Benjamin speaks of 'the New Jim Code' and points out that racist processes of segregation and territorial stigmatisation are creeping back in via digital surveillance methods. Benjamin writes, 'The power of the New Jim Code is that it allows racist habits and logics to enter through the backdoor of tech design, in which the humans who create the algorithms are hidden from view' (2019: 160). Yet this algoracism is barely recognised or penalised as violence, if at all.

By shifting our understanding of AI and algorithms from the intangible to the material, the question of our relationship with AI and algorithms also becomes a political one, as it addresses the formation of relations to oneself and to others through algorithms. This is what political geographer Louise Amoore calls the 'ethicopolitical condition we must live in' (2020: 19). In many cases, hypernudges will have manipulative features because the stimulus takes on the form of an instruction and such nudges target cognitive processes over which people have barely any control. This can take on innocent forms and serve noble ends, as in the case of zebra crossings and streetlights that light up automatically when pedestrians pass by, indicating the

safest walking route in residential neighbourhoods and university campuses. But the use of hypernudges becomes questionable when personal data is collected on a large scale, without people's knowledge or consent.

An example is football stadiums, where techniques of algorithmic psychopower are deployed specifically to eliminate racism and discrimination. In Dutch stadiums, smart microphones are hung above the boxes with the most fanatical fans, recording their chants to listen for racist language. This so-called 'mood detection', in which the supporters' moods are divided into seven categories from 'really happy' to 'really angry', determines when the atmosphere in the stadium needs changing. The intervention is ever further perfected by measuring its efficacy and feeding it back to adjust the intervention. When the software recognises a problem such as racist songs, positive chants are automatically displayed on billboards to influence the mood of the stadium. Sorama, the technology company responsible for the application, states, 'The software recognises particular tunes and displays positive chants to go with them, so that these gain the upper hand.'[3]

A third and final example of algorithmic psychopower is symbolic for the way a positive atmosphere is also becoming the norm in public spaces. Besides colours (navigation app Waze) and sounds (football stadiums), scents can also be used for behaviour manipulation and restriction. For instance, Stratumseind, a 300-metre-long street of pubs and clubs in the Dutch city of Eindhoven that attracts 15,000-20,000 young people at weekends, has experimented with emitting a calming and

peaceful scent of oranges to reduce aggression and increase a sense of security. The amount, colour and intensity of light is also constantly adjusted to make the area safer, livelier and more attractive. The colour blue is said to have a cooling effect. A certain shade of blue can lower the heart rate, which is useful for reducing aggression. In order to be able to intervene at any moment with colours and scents, large volumes of data are collected on social interactions, police presence, waste in the street, noise levels, weather information, parking density, beer consumption, young people entering and leaving Stratumseind, and social media messages among other things (Schuilenburg & Peeters, 2018; Pali & Schuilenburg, 2020). AI and algorithms thus help smoothly alter the atmosphere in such spaces in ways that move and affect people, placing us in a different relationship with ourselves and others and raising the question of how freely and anonymously we can still move in public.

In short, the history of surveillance consists of a long series of social and technological changes and of things people want to do with technology. First, surveillance made people visible – and therefore governable – on a large scale, from censuses in the nineteenth century to camera monitoring in the twentieth. Over time, the role of technology has changed and now the next development presents itself in the form of algorithmic psychopower and hypernudges to model the behaviour of individuals and groups, in a manner reminiscent of George Orwell's *Nineteen Eighty-Four* and his observation that the only privacy to be found is in your own head: 'Nothing was your own except the few cubic centimetres inside your skull (1984: 23)'.

The intentions behind the forms of psychopower discussed here are undoubtedly good, but if we value our internal lives, then protection against unwanted external influences must be robustly improved. This may include a right to mental integrity and its protection through the right to mental privacy.[4] In the case of psychopower, emotive temptation by means of AI and algorithms, the question, after all, is no longer 'who you are' but 'how you feel'.

3 Big Data Policing

3.1 Introduction

Of all the motives for using AI, a starring role goes to what I referred to in chapter 1 as driving principles. A great deal of weight is given to efficacy and efficiency in introducing AI applications to completely different sectors of society, such as mobility, care and education. In contrast to chapter 2, in this chapter I specifically focus on the use of digital surveillance in the investigation and management of crime and antisocial behaviour. The increased scale and depth of this phenomenon can be explained by the emphasis in our society on innovation in technology itself, which must then be broadly applied. This has to do with factors such as political discourse and cultural aspects, with views on how secure or insecure citizens feel, and a great deal of political support for preventing risks as early as possible by technological means. Frank Pasquale writes in his book *New Laws of Robotics*: 'A mix of drones, CCTV cameras, and robots may be far less expensive than battalions of police officers. They may be more effective, too, and even less likely to injure suspects or wrongly target the innocent' (2020: 122).

I would term this 'innovation realism' – ideologically charged political choices in the guise of inevitable technological processes. In other words, the political and cultural context in which digital surveillance takes place, which in the security domain increasingly stands for risk management and the consequent precautionary thinking, is at least as important (e.g., Garland, 2001; Schuilenburg, 2015).

Driven by fear of crime and antisocial behaviour, be it well-founded or otherwise, society has been taken over by an unfettered need to manage and limit risks in order to guarantee security. People speak of 'governing the future' and a 'pre-crime society' (Zedner, 2007), in which we no longer punish crimes that have been committed, but instead prevent potentially risky behaviour. The government plays an important role in ensuring the security of society, and one of the consequences of this is the tendency to want to deploy criminal law as early as possible in order to prevent all kinds of risks, an issue termed 'the flight forward' by jurist Matthias Borgers (2007). To put it simply, in traditional criminal law there was first suspicion and then surveillance; now there is surveillance followed by suspicion. Add to this the belief that everything can be captured in big data and algorithms and that security issues can be more effectively and efficiently tackled with the latest technological gadgets, and all this results in substantial faith in AI as the number one solution for the security problem (Morozov, 2013).

The reason I wish to discuss the use of AI to investigate and tackle crime and antisocial behaviour is that criminology has so far paid hardly any attention to the digitalisation and algo-

rithmisation of the security problem. Given the pace of current technological developments in AI, this may not be surprising, but as a result there is not yet a good overview of which parties are deploying digital applications in the detection and prevention of crime and antisocial behaviour. Looking ahead to the next section, I can state that the literature on this topic is mainly restricted to the phenomenon of predictive policing, where the police attempt to predict whether there is a raised risk of crime in a particular time or place, and also whether individuals have a higher chance of becoming involved in a crime, as a perpetrator or a victim, in order to then deploy surveillance accordingly (Perry et al., 2013; Ratcliffe, 2014; Hardyns & Rummens, 2017). Besides American systems such as PredPol and HunchLab, comparable applications are also used in countries such as Germany (KrimPro and Precobs), Italy (KeyCrime) and France (Maprevelation). In the Netherlands, the national police force has been working since 2017 with the Crime Anticipation System (CAS), which predicts where and when there is a raised risk of certain forms of crime.

However, various examples from the previous chapters – from the smart Amazon doorbell Ring to the Sentry Mode in Tesla cars – show that it is not only the police who are involved in making society secure and using AI tools to do so. This raises the question of whether criminology takes an overly limited and one-sided view of the range of parties active in this area and of the applications being used.

3.2 Big data policing

In this section I focus on the phenomenon of big data policing, which I defined in the first chapter as follows: the use of large volumes of data made accessible by algorithms with the aim of making society safer and more liveable.[1] This requires surveillance activities during which data is collected. I distinguish here between parties involved in big data policing 'above', 'beyond' and 'below' the police. Here it will suffice to describe the main developments and applications, with a focus on the Dutch security industry. It should be noted that in practice, the parties distinguished as being *above*, *beyond* or *below* the police often overlap.

a. Big data policing by the police

The rise of big data policing by the police force fits into a historical perspective of improving police performance using data and statistical methods. The most important and most frequently used source is data acquired by the police in carrying out their own duties. This includes information from police reports, material such as images and fingerprints, telecommunications data, and information generated by more recent digital surveillance technologies and innovations, such as automatic facial recognition. The collection and processing of data by the police in carrying out their duties first began in the nineteenth century, when police forces became more intensively engaged in setting up large archives of mug shots and fingerprints (dactyloscopy) as a record of people who had come

into contact with the police before. These archives are used to register people's unique characteristics and to exchange information between police forces domestically and internationally (Sekula, 1986; Hausken, 2016; Leloup, 2023), but also make it possible to conduct scientific research into many issues – for instance, whether features of a person's appearance can be used to distinguish criminals from non-criminals.

Besides the growth of photographic and other data, in the nineteenth century statistical techniques were applied for the first time that revealed patterns of crime and differences in time and place. Well-known names in this field include the Belgian astronomer and demographer Adolphe Quetelet and the French jurist André Michel Guerry (Morrisson, 1897; Beirne, 1987). Processing information with the right techniques allows users to discover underlying patterns, including trends in time and correlations between different criminological phenomena. For instance, in *Essai sur la morale de la France*, published in 1833, Guerry points to similarities in crime figures between different regions in France when it comes to proportions of different groups of the population, gender and age, in the distribution of types of criminal offenses over the year. He looks for explanations in socio-economic factors such as poverty, but also pays plenty of attention to circumstances such as work and education.

Another important development in data-driven police work is the phenomenon of 'actuarial justice' or 'risk justice', which arose in the last two decades of the twentieth century and in which attempts were made to predict the risk of criminal

behaviour using techniques from the insurance world (Simon 1987; 1988; Feeley & Simon, 1994; Ericson & Haggerty, 1997). Such techniques included identifying and classifying people based on different grades of risk, with the aim of preventing actions and behaviour that could present a threat to a secure society. Starting from the thesis of the German sociologist Ulrich Beck on the risk society, in their classical book *Policing the Risk Society* (1997) Richard Ericson and Kevin Haggerty refer to police personnel as 'information managers', showing how the police force is transforming through new surveillance technologies, from the police car ('mobile offices and technological laboratories') and the relationship with citizens ('making up communities') to the bureaucratic police service ('new hierarchies of expertise are formed, including an enhanced place for computer specialists').

The next step towards big data policing by the police force is developments such as intelligence-led policing, where decisions are made based on analysed data and knowledge for the conduct of police work and more proactive anticipation of certain forms of criminal activity and antisocial behaviour (Ratcliffe, 2016). In *The Technology of Policing* (2008), Peter Manning points to the long history of 'crime mapping' and 'crime analysis', from the city diagrams of the Chicago School at the beginning of the twentieth century through to the introduction of new tools such as Compstat ('Computer Stats') in order to gain information on crime in large city neighbourhoods faster and more accurately and take targeted action, for instance conducting more frequent and intensive surveillance in places where

more crime occurs, such as blocks of flats or parks ('hotspot policing').

The digitalisation and algorithmisation of society are further increasing opportunities for the police to collect and process data. Based on her research into big data policing by the Los Angeles Police Department (LAPD), Sarah Brayne concludes that in American police practice, 'data are used for predictive, rather than reactive or explanatory, purposes' (2017). Recent research into big data policing by the Dutch police, however, shows that applications in this area are deployed far more broadly and differ in function and complexity (Schuilenburg & Soudijn, 2023). Besides the investigation of crime and use in intelligence, traditional enforcement in the street also systematically employs big data applications. What stands out here is that predicting crime is actually the *least* conventional use. In fact, big data applications in Dutch police practice are mainly used for internal and administrative processes, and when it comes to intelligence and investigation of crime, they're not used predictively but in real time and retrospectively.

In the case of real-time support, applications are used to reduce the burden on police capacity and accelerate police work, but also to process information that could not be managed in a timely fashion if it were only processed by humans. An example of this is Automatic Number Plate Recognition cameras which can compare the number plates of passing cars with those recorded on a reference list ('hit') of vehicles wanted by the police, for instance because they have been used for ram-raiding. In the street, police officers have access on their smartphones

to various linked police apps that tell them where a suspect is, whether they are armed and dangerous, how groups of rioters are moving through the city and what is happening on social media.

Retrospective applications can include applications in criminal investigations, particularly when large volumes of data need processing, such as reading millions of intercepted crypto communications from the chat service EncroChat that is used by criminal organisations. Algorithms trained on different language models and labelled indicators can filter the data by priority (which messages need reading first) and rapidly find connections that are relevant for the investigation of an issue such as money laundering or human trafficking. In this way, the data storage devices that are seized are effectively rewound and big data applications function like a time machine that lead the police to the past rather than to the future.[2]

The same empirical research reveals that Dutch police practice is largely about relatively simple big data applications, such as investigative apps with simple, rule-based algorithms for street work or linking and unlocking large databases. In other words, there is no question of complex, advanced data-processing models or self-learning applications that adapt their rules on the basis of learning experiences or act completely autonomously (i.e., without human intervention). In sharp contrast with all the ominous science-fiction-inspired media stories about a devastating AI super-intelligence that supersedes humans across the board and makes them completely superfluous, these are

very weak forms of AI, where algorithms are not given a free hand but are approached by means of certain hypotheses.

b. Big data policing above the police

Big data policing is not only conducted by the police in the context of performing their duties – in recent decades, applications in this area have also been exploited by diverse organisations operating above the national level. Transnational big data policing (Sheptycki, 2000) is done through collaboration between nation states at an international level. A current example is the Prüm system, a European network set up for the automated exchange of fingerprints, DNA profiles and information on motor vehicles (Neiva, Rafaela & Machado, 2022). Elizabeth Joh (2014) calls DNA databases one of the three most used applications in big data policing, besides crime prediction and mass surveillance. The Egmont Group of Financial Intelligence Units, an international collaboration focused on improving international data exchange between national financial intelligence units, is another example of big data policing 'above' the police. In a briefing, the Egmont Group indicate that they are involved in 'incorporating different digital tools to assist their operational efforts. These tools range from automation to the use of large datasets, big data and advanced analytics such as artificial intelligence (AI) and machine learning.'[3]

Big data and algorithms also form important spearheads in the European Union's Security Strategy (2020-2025). For instance, the European Union states that 'artificial intelligence,

space capabilities, Big Data and High Performance Computing are integrated into security policy in a way which is effective both in fighting crimes and in ensuring fundamental rights'.[4] They refer to risks from terrorism, organised crime, drug dealing, human trafficking and cybercrime. Transnational big data policing is also conducted by supranational organisations such as EuroJust and Europol. The analytical capacities of Europol, for instance, are deployed in areas such as 'cybercrime, terrorism-related propaganda, enhanced risk entities solution (ERES), open-source information (OSINF) and open-source intelligence (OSINT)' (Hoek & Stigter, 2021: 25). Europol has also set up the Europol Information System (EIS), which is filled with data from national police organisations from the European Union.[5] As a final example, databases for border control in the European Union, including the Schengen Information System (SIS), are the most used and largest information exchange system for security and border control in Europe.

c. Big data policing beyond the police

Big data policing is also carried out by parties operating 'beyond' the police, which play an increasingly important role in security management. Both public (local councils and special investigation services) and private parties are developing ever more digital activities to make society more secure. Various Dutch local councils, for instance, use investigation tools to predict crime and other risky behaviour including fraud scorecards and welfare algorithms to investigate fraud around social provision, in which specific target groups are being labelled

risk groups. Many private parties, from Google to Tesla, also work in security using large datasets and algorithms and following their own guidelines. 'Our mission to reduce crime in neighbourhoods has been at the core of everything we do at Ring,' claims Jamie Siminoff, former CEO of Ring, which now belongs to Amazon.[6]

Buy an electric car from Tesla or the smart doorbell Ring from Amazon and you get free surveillance along with it. If you switch on Sentry Mode, the four cameras on the outside of the Tesla standardly record images if the car 'notices' danger. Suspicious persons are filmed and when the Tesla is parked in front of someone else's house, it also makes it possible to see what the residents are doing inside.[7] With a premium connectivity subscription, the camera images can be streamed live on the Tesla app. A wireless connection between the app and the car enables the Tesla owner to install all the latest functionalities in their vehicle, with which they can not only monitor themselves ('selfveillance') but are also watched by the company, which collects all the data on a platform ('coveillance'). This makes it possible to monitor the preferences of drivers as a basis for Tesla to develop new products and services as well as targeted marketing, including discounts on insurance premiums for a 'safe' driving style. On the Amazon Ring, neighbourhood residents anonymously share video images recorded by the Ring Doorbell through the social media app 'Neighbours'. Meanwhile the company Ring is working on a facial recognition system that gives a signal through the 'watch list' function when a 'suspicious' person is recognised on the doorbell's camera images.

All this raises the risk of what I call 'surveillance feudalism' or 'feudal security'.

The work of authors such as Yanis Varoufakis and Jodi Dean is helpful in comprehending the relationship between feudalism and surveillance. They describe society in terms of techno-feudalism, whereby a very small elite of tech companies have become so large and influential that they wield complete control over the markets. However much the activities of companies such as Amazon, Airbnb and Deliveroo may differ from each other, they share the characteristic of bringing together supply and demand on digital platforms. This represents a shift in value extraction from tilling the land to selling on markets and finally to the cloud. Yanis Varoufakis, former Greek Minister of Finance, writes, 'Today, it is cloud-based capital, or cloud capital in short, that grants its owners hitherto unimaginable powers.'[8]

The roots of techno-feudalism go back to the feudal power of noble landowners in the Middle Ages, when simple peasant farmers toiled under the most deplorable conditions, working long days with few alternatives. The successors of the medieval feudal lords are companies such as Uber and Airbnb, and the working conditions of their personnel strongly resemble those of the medieval peasants. Platform workers such as taxi drivers, domestic staff and food delivery workers are not on permanent contracts and their labour is poorly remunerated. They always have to be on call, accrue no pension and barely have opportunities for continuing education. Add to that feelings of monotony and alienation, along with the limited influence platform

workers can exert on their working conditions, and society has acquired a new underclass.[9] The American political scientist Jodi Dean blames this alienation on the trends of digitalisation and algorithmisation which have contributed to the growth in power of companies such as Uber and Amazon. Dean (2022) writes, 'If feudalism was characterized by relations of personal dependence, then neofeudalism is characterized by abstract, algorithmic dependence on the platforms that mediate our lives.' Among other things, the tech companies use algorithms for tasks such as staff management, leading to a lack of transparency as to how decisions are reached and personal data is used.

Another major influence is the fact that platform companies also use big data and algorithms in the field of security. When you visit the platforms for Airbnb and Booking.com, you're instantly entering the world of digital surveillance: everything you click on is also registered and retained for security purposes. After all, these platform companies don't just offer services for searching for a place to stay the night – the hotel has also become a way of collecting personal data, scoring people based on their behaviour and experimenting with automated decision-making (including profiling based on particular categories of personal data). In doing so, tech companies such as Amazon (originally a bookshop) and Google (originally a search engine) offer technological solutions to social problems, increasing the potential of big data policing. For instance, these companies look at urban areas from the perspective of improving security in entire neighbourhoods with data and sensors. Google has become notorious for its now discontinued role in a development project to transform a dilapidated waterfront area in

Toronto into a smart neighbourhood using sensors and cameras to register not only traffic and air quality but also to continuously monitor residents' behaviour to make the area safer. I would call this 'surveillance feudalism'.

Surveillance feudalism also takes place closer to home. Smart gadgets with inbuilt cameras, directional microphones and tracking devices inside houses record images and sounds all day long for the residents to view in real time or retrospectively. In order to prevent burglary or track down burglars faster, these devices can be linked – all the better for protecting your house from people of whom you don't know what to expect. As an example, the Amazon Ring security camera and sound detector on the smart loudspeaker Amazon Echo Dot are linked to the smart home platform Amazon Alexa – a cloud-based voice service to operate all the smart household devices. This effectively turns your house into a digital fortress and reduces social cohesion in the neighbourhood to digital interaction.[10]

d. Big data policing below the police

Besides governments and companies, citizens also use big data applications to improve security. With more than 10 million users, the Citizen security app (previously called Vigilante) is one of the most downloaded apps in the United States. Citizens can use the app to report criminal activity and receive announcements about crime, accidents and other dangerous occurrences in their neighbourhood. More and more citizens worldwide are patrolling in neighbourhood prevention teams,

and in doing so they make use of specially designed apps with neighbourhood functionality – alongside well-known apps with group functions such as Telegram and WhatsApp. Some apps have a broad purpose, as in the case of Nextdoor, which shares messages on crime prevention, lost pets or free items. Other apps are specifically developed to improve security in the neighbourhood, as in the Dutch case of 'Veiligebuurt' (which means 'secure neighbourhood'). In the most advanced apps, sensor data from intelligent cameras and sound sensors in the area are used to indicate 'suspicious' movements.

These kinds of 'non-police databases' (Brayne, 2021) are often larger and more varied than the previously mentioned police data and contain qualitative data that can be used by the police in carrying out their duties. Various examples show that the information on these apps is shared liberally and rapidly with the police when it comes to serious offenses. Meanwhile the Amazon Ring Doorbell has been working with more than 4,000 American police forces, giving the police access to images on the Ring platform, without any clear legal control. Dutch citizens with a security camera can voluntarily register with the 'Camera in View' initiative, a police database in which more than 55,000 cameras belonging to citizens are registered for the police to call up images if a crime is committed in the area.

Horizontal surveillance, too, can have many unwanted side effects such as vigilante justice, overreaction to insignificant risks and automated ethnic profiling, when individuals are labelled suspicious based purely on external characteristics, from youths in hoodies covering their eyes to young men with dark

skin and beards (Dixon, 2017; Mols & Pridmore, 2019). At the same time, it seems that neighbourhood crime prevention through 'do-it-yourself surveillance' groups tends not to provide major clues that reduce the level of crime or increase the sense of security in the area. There are indications, however, of an increase in willingness to report and the positive experience of more direct connections with the authorities (Eysink Smeets et al., 2019). Besides a better relationship with the police, digital crime prevention on a local level can have a positive effect in strengthening bonds between residents, which increases social cohesion in the area (Van Steden & Mehlbaum, 2021). Residents get to know one another better and this can lead to more in-person contact in the neighbourhood.

3.3 Double-edged sword

When we examine critical reactions to the use of AI and digital surveillance by police and other parties for security purposes, we find an accumulation of arguments that have been used for some time against all kinds of control and coercion. The emphasis is on the secretive and large-scale character of surveillance and, in conjunction with that, the infringement of citizens' privacy. Some nuance is nevertheless required. In chapter 1, I touched on the etymology of the word 'surveillance' and its various meanings. The French word *surveiller* is derived from the Latin *vigilāre* ('to keep watch' or 'to guard'), which comes from *vigil* ('vigilant' or 'alert'), which in turn can be derived from *vigēre* ('to be vigorous'). *Veiller sur* means 'watch over', implying both 'control' and 'care'. David Lyon sums up

the different meanings as follows: 'Surveillance both enables and constrains, involves care and control' (2001: 3).

The positive meaning of care has connotations of connectedness and responsibility. Gary Marx uses the term 'positive surveillance' (2016: 231), pointing to the care of parents for the development of their children and that of doctors for their patients, through diagnosis, treatment and monitoring. In *Theological Perspectives on a Surveillance Society*, Eric Stoddart derives the notion of care from Christian ethics, arguing that it goes beyond goal-oriented action or technological possibility, and writes that 'to neglect aspects of these responsibilities in parenthood, education, health and even friendship, is to be less than a faithful parent, teacher, doctor or companion' (2011: 3). This positive side of surveillance – which points to a concept derived from a pastoral power and the figure of the shepherd, that can be traced back to early Christianity and even to the pre-Christian Eastern world – indicates a more inclusive and affirmative approach to security which I will examine in greater detail later on.

For now, the key point is that the positive and negative sides of surveillance cannot easily be separated, making it necessary, as I showed in chapter 2, to determine in a given context which aspect is likely to gain the upper hand. An illustrative example of the double-edged sword of surveillance is the Pegasus scandal, where espionage software developed to investigate terrorists and serious crime was used by governments to pursue political opponents, journalists and human rights activists by reading messages on their phones. In other words, software

that was intended to enable a secure and free society ended up being misused for the suppression of independent thought and free speech. The double meaning of surveillance is also apparent from the more innocent example of the baby monitor with which parents can always see what happens in a baby's room. The underlying idea is care for the infant – but when the baby has grown into a teenager and owns their own mobile phone, the parents can continue to monitor them through GPS to check whether they are playing truant. This raises the other side of surveillance – from one moment to the next, care becomes total control and intrusion. All this means that there is often a notion of *dual use* in surveillance. The same surveillance technology can be used for completely different purposes. In terms of AI: it can be used for bad or for good.

I take digital surveillance to be a *pharmakon*, something that is simultaneously medicine and poison, with powers both to heal and to make people ill. In his essay *Plato's Pharmacy*, the French philosopher Jacques Derrida points to the contrary meanings of the Greek word *pharmakon*: '"remedy", "recipe", "poison", "drug", "philter," etc.' (1993: 71; see also: Stiegler, 2012). The combination, the fact that everything to do with technology can be both poison (problem) and remedy (solution), first arises in Plato's dialogue *Phaedrus*, which recounts the origin myth of writing and its detrimental effect on memory. Writing is termed a 'pharmakon' here: its invention makes people wiser, but it can also lead to forgetfulness because people no longer exercise their memory when they learn to rely on technological tools. As Socrates puts it, 'What is the propriety and impropri-

ety in writing, how it should be done and how it is improper?' (Plato, 1999: 71, 274 b).

Socrates' question is still surprisingly relevant because it draws attention to the issue of how AI can be deployed with 'the right care'. How may surveillance be performed positively, for the common good? AI can be useful, for instance when the police deploy big data and algorithms to combat organised crime such as human trafficking, but it's toxic when it leads to systemic violations of fundamental human rights. A topical illustration is the use of surveillance on the external borders of Europe in repelling and selecting refugees and migrants. This area appears to serve as a testing ground for the latest digital technologies, including 3D radar systems, sensors to detect mobile phones and biometric applications, giving rise to recurrent accusations regarding so-called 'pushbacks' – the practice in which refugees are not given a chance to claim asylum in a European country because they are forced, often violently, to return to the place they came from.[11] This brings me to the question of how ethics and the democratic rule of law can keep investigative applications in big data policing controllable. But first, I'd like to present a list of films, books and TV series on AI and digital surveillance.

Interlude III. Films, Books and TV Series

AI and digital surveillance are rewarding subjects for literature and film. For a long time, books have been written and films made about intrusive forms of control and our realistic and unrealistic fears about everything to do with technology. The following is a brief selection of the best films, TV series and books I have watched and read on the subject.

Literature

1. *Bot* – Charles den Tex (2016)
   Dutch thriller about Bas Portier, a hyper-intelligent young man in love with a Chinese-Dutch woman, T-Li, who is as much of a nerd as he is. Portier is asked to build an information system, but when his client dies, no one is able to unlock the system anymore. A tense story about the world of codes and formulas. On writing the thriller *Bot*, Den Tex says, 'I gathered together a number of ideas on how you remain yourself amidst the strong currents of family and the information society.'

2. *Frankissstein: A Love Story* – Jeanette Winterson (2019)
   The book begins in 1816, when five people go on holiday to Lake Geneva: the poets Alfred Lord Byron and Percy Shelley, Shelley's wife Mary, her half-sister (and Byron's mistress) Claire, and Byron's personal physician Polidori. During the holiday, Mary Shelley gains inspiration for her famous story *Frankenstein*, on the creation of a non-biological life form. Besides gender fluidity, recurrent themes in Winterson's book are the opportunities and threats of AI. The author illustrates beautifully how the discussions around new technology are common to all eras, from the Luddites who protested against the weaving machine and broke into factories to destroy them, to today's debates around whether AI is making humans superfluous.
3. *Klara and the Sun* – Kazuo Ishiguro (2021)
   Novel about the robot Klara who takes care of Josie, a sickly 14-year-old girl, acting as a kind of butler and attempting to serve her as well as possible. Klara constantly observes and learns from what she sees. She also practises empathy, because otherwise she can't help Josie properly. Ishiguro cleverly plays with the question of whether empathy is something typically human or can be learned by a robot placing itself in the shoes of someone else.
4. *Machine Like Me* – Ian McEwan (2019)
   This novel by the British author Ian McEwan takes place in the early 1980s, but soon transpires to be set in a kind of parallel universe. *Machine Like Me* is a futuristic novel set in the past: The Beatles are back together, Alan Turing – the ingenious mathematician – is still alive, and self-driving cars are everywhere. In the story, the main character

Charlie spends 86,000 pounds of his inheritance on a robot named Adam, who can barely be distinguished from a human. A love triangle emerges between Charlie, his girlfriend Miranda and Adam. When Miranda is 'unfaithful' to Charlie with Adam, Charlie can still smell 'the scent of warm electronics on her sheets' days later.

5. *The Memory Police* – Yoko Ogawa (2021)
   What does it mean when our memories of things are banned? *The Memory Police* is set on an island where all kinds of things are disappearing by decree, and people's memories of those things also evaporate. When the birds disappear, the main character says, 'I realized that everything I knew about them had disappeared from inside me: my memories of them, my feelings about them, the very meaning of the word "bird" – everything.' Barely any resistance is shown in the book, making it a novel about surrendering to destiny.

Films

1. *Code 46* – Michael Winterbottom (2003)
   Science fiction film by the British director Michael Winterbottom, who was also responsible for the catchy music film *24 Hour Party People*. *Code 46* is about a society that is sharply divided in two. In Winterbottom's sketch of the future, the uninsured in society are banished to the deserts, vast plains between the heavily guarded cities. When people want to travel between cities, they have to take out insurance, the so-called 'papelles' – a combination of a visa and a DNA passport. No insurance means no movement.

Featuring Mick Jones from The Clash singing 'Should I stay or should I go?' in a karaoke bar.

2. *The Lives of Others* (Original title: *Das Leben der Anderen*) – Florian Henckel von Donnersmarck (2006)
   Penetrating view of the paranoia in communist East Germany in the early 1980s. From the capital East Berlin, the Stasi security service, embodying the eyes and ears of the country, is constantly looking over everyone's shoulders. In the film, Gerd Wiesler – working for the Stasi – is tasked with spying on the artist couple Georg Dreymann and Christa-Maria Sieland. Along the way his faith in East German socialism and the use of the Stasi crumbles. In an interview about the film, director Henckel von Donnersmarck states, 'If your parents think you're hiding something under your clothes, they can ask you to take your clothes off. A totalitarian system does the same.'
3. *Gattaca* – Andrew Niccol (1997)
   The film is an intelligent combination of science fiction, drama and thriller. The story is set in a society in which people can have perfect children through genetic manipulation. All traits can be carefully selected and all genetically determined diseases have disappeared. Anyone who was born naturally – and is therefore genetically inferior – is fated to live as a second-class citizen in the underclass, cleaning and scrubbing the space station Gattaca. The film raises questions on issues such as freedom, identity and justice. To what extent do your genes determine your fate? Ethan Hawke plays the lead, with supporting roles for Uma Thurman, Jude Law and others.

4. *Her* – Spike Jonze (2013)
   A love story in which the lonely divorced writer Theodore Twombly, played by Joaquin Phoenix, falls in love with his new computer's operating system. The system has a name: Samantha. It's smart and funny and adorned with the sultry voice of Scarlett Johansson. Samantha turns out not only to be a useful personal assistant, but also to have all kinds of feelings and interests. Director Spike Jonze cleverly plays with the personal relationship between human and machine, invoking themes such as intimacy, veracity and emotions.
5. *Minority Report* – Steven Spielberg (2002)
   'In our society we have no major crimes,' says police commissioner John Anderton (Tom Cruise), 'we have a detention camp full of would-be-criminals.' In the literature on predictive policing, references to *Minority Report* have become the norm. Nevertheless, the film is too interesting to be dismissed as a cliché. Note, for instance, the procedural rules when the precogs predict a murder. The head of the Pre-Crime Unit, John Anderton, has to read out the names of the victim and the culprit to two witnesses, Dr Katherine James and Chief Justice Frank Pollard. The entire procedure is filmed and James and Pollard check whether the names read out match those carved into the precogs' wooden balls.
6. *Red Road* – Andrea Arnold (2006)
   The main character Jackie, played by Kate Dickie, works as a security official for the local council. She earns a living from examining security camera footage to see if anything is happening around the grim and gloomy flats of Red Road in the north of Glasgow. When Jackie recognises the man in

the images who is responsible for the death of her husband and children, she doesn't inform the police but investigates for herself. She becomes the embodiment of a camera, and monitors Clyde, played by Tonny Curran, by completely taking on the function of surveillance technology and watching him 24 hours a day. As in Franz Kafka's famous story *The Metamorphosis*, we see Jackie gradually change as a result.

7. *THX-1138* – George Lucas (1971)
   The visually striking debut of the American director George Lucas about a world in which inhabitants are numbered and followed on camera 24 hours a day. The use of sedatives to suppress emotions is compulsory. Inspired by books such as *Brave New World* (1932) and *Nineteen Eighty-Four* (1948), Lucas used his film for incisive criticism of 1970s consumer society. One of the best scenes in the film features the 'white void', the prison where main character THX-1138 is detained in a shapeless in-between world.
8. *Videodrome* – David Cronenberg (1983)
   Canadian body-horror about a cable television producer, played by James Woods, who discovers a snuff film channel called Videodrome. When Max Renn sees his sadomasochistic girlfriend Nicki Brand, played by Blondie singer Deborah Harry, auditioning for Videodrome, he starts hallucinating and develops an organ in his stomach to take in video cassettes. After more than 40 years, the film continues to make for thought-provoking viewing, particularly because of the way reality and appearance constantly overlap and Cronenberg beautifully illustrates how our bodies are influenced by the latest technology.

TV series

1. *The Capture* – Ben Chanan (2019)
   Six-part British thriller series about CCTV intended to keep the streets of London safe. The plot centres on an Afghanistan veteran who has been acquitted of murdering a Taliban terrorist but is now suspected of sexual assault and abduction of a human rights lawyer. The crime is recorded on security cameras, but investigator Rachel Carey, beautifully portrayed by Holliday Grainger, increasingly doubts the reliability of the video images. It soon emerges that the images have been manipulated and don't tell the truth. 'Seeing is deceiving', as the series slogan states.
2. *Black Mirror* – Charlie Brooker (2011 – today)
   Award-winning series about the relationship between technology and unease in our digital society. The title refers to the screen of a TV or mobile. Shane Allen, head of comedy at the BBC, calls the series 'a satirical drama for the social-media generation'. One of the best episodes is about a young woman obsessed by her social rating. In the story, titled *Nosedive*, socially desirable behaviour leads to higher ratings: to enjoy luxurious living quarters or dining out in high-end restaurants you have to score at least 4.5 points, while falling below 2.5 makes you part of the social underclass. Lacie just doesn't manage to get a 4.5 rating, which means she can't get her dream apartment. Eventually she ends up in prison, far from the hungry monster of surveillance capitalism in which everything revolves around getting people to hand over personal experiences free of charge to be translated into behavioural data.

4 From Reaction to Direction

4.1 Introduction

It's easy to get lost in all the promises of AI and digital surveillance. New technologies are penetrating security practice at an ever faster pace, making ambitious promises. Who would not be impressed by the technical capabilities of the latest gadgets in big data policing? But besides enthusiasm for the benefits AI can offer, digitalisation and algorithmisation of criminal investigation and law enforcement also raise many legal and ethical questions. For instance in crime prevention by the police and local authorities, which ranges from systems that contain invisible algorithms to investigate tax fraud, through so-called 'testing grounds' in which 'suspicious' car movement patterns are registered to combat mobile banditry, to the monitoring of individuals based on the colour of their skin in risk-oriented border controls by the Royal Netherlands Marechausee. This is just a small selection of examples that have caused commotion in recent years over a government trying to make society secure and more liveable using technological applications.

Powers of investigation and control intrude deep into fundamental constitutional and human rights, and the application of those powers must be governed by public safeguards, including the principles of proportionality and subsidiarity. In that respect the European Union – unlike the United States and China – increasingly fulfils a regulatory role in legislation with respect to the digitalisation of the security issue.[1] Thus the European Commission, which is responsible for European legislation, has set up a large number of legal frameworks for big data and algorithms, including AI technology (AI Act) and digital services (Digital Services Act). With respect to law enforcement, the Regulation on a European Approach for Artificial Intelligence (AI Act) classifies AI systems, imposing stricter rules the greater the risk of the associated technology.[2] AI systems that are determined to be 'high risk' (Annex II) are used by the police and judicial authorities, among others. When it comes to police use of big data, this comprises AI applications used for (i) predicting an actual or potential crime, (ii) profiling individuals when investigating crimes, and (iii) crime analyses in which large quantities of data are searched to identify unknown patterns or discover hidden relationships.

On a national level too, the use of AI by the police increasingly receives the legal attention it deserves. However ground-breaking the latest technology in this area may be, it can have significant implications for the individuals against whom it is used. Hence the need for sufficient legal guarantees that new AI technologies that are desirable from an investigative perspective do not violate the rights and freedoms of citizens. Underpinning

principles such as the right to privacy effectively function as a healthy counterweight to the driving values of security and efficiency. In the EncroChat case, in which over 115 million cryptophone messages from users were intercepted, the Dutch court judged that there was no question of serious violations of the principles of due process (Schermer & Oerlemans, 2022). Recently, proposals were also made to modernise the Dutch Code of Criminal Procedure to enable it to better adapt to new technological developments in the investigation of crime and antisocial behaviour and enforcement of the law (Commissie Koops, 2018). The new code pays more attention to regulating new investigative powers in a digital environment, including closer regulation of systematic research in public sources and research into seized digital devices containing data such as smartphones and computers.[3]

Although nationally and internationally there are more and more developments to maintain control of the digitalisation and algorithmisation of police work, the question is whether these sufficiently protect the rights of citizens. From a public perspective, on the one hand, it's important that investigation and law enforcement can benefit as much as possible from new AI resources. On the other hand, however, these technologies should be kept manageable and controllable within a framework of values important to our democratic society. For a good understanding of this point, I focus in this chapter on the legal and ethical dimensions of making surveillance public.

4.2 Legal questions

In order to gain a better understanding of the legal issues at play in AI and digital surveillance by the police, it is instructive to draw a distinction between the *input-*, *throughput-* and *output* of a specific application (Peeters & Schuilenburg, 2023). *Input* refers here to the datasets used, from found data (collected through a passive, non-observational process) to automated data (automatically and inherently generated by surveillance devices and systems). *Throughput* is focused on the processing of data by algorithms through browsing, ordering, analysing or linking it to other data.[4] All this results in a concrete decision or a recommendation for one or more actions – the *output*.

In the following sections, I give a broad outline of the key legal issues that play a role in each of these three stages. It strikes me that the legal debate on data-driven investigation mainly focuses on the processing of data (*throughput*). In practice, as I showed in chapter 2, the three stages constantly overlap, forming a digital control loop, and therefore need examining in combination.

a. Input

A first legal issue relates to the importance of using what's known as 'clean data' for criminal prosecution purposes (Richardson, Schultz & Crawford, 2019; Das & Schuilenburg, 2020). After all, the principle of 'garbage in, garbage out' applies to all data systems; if dirty data enters the analyses, the results will also be

contaminated. Since the input is the foundation of any decision or advice in the criminal prosecution context, but also in intelligence work or advice to the judge in sentencing, data that is itself erroneous can lead to an output in the form of decisions or recommendations of actions that are also problematic. This is the legal problem of 'dirty data'. In the broadest sense, this is about data garnered from police action that is either illegally obtained or incorrect. Illegally obtained data might involve infringement of rules for obtaining the data, for instance by the violation of legal standards, provisions from the European Convention on Human Rights or unwritten standards, including the principle of due process. A current example is data that comes from or is derived from biased or criminal practices, such as discrimination by police officers in identity checks, searches, arrests or other forms of illegal behaviour by investigative authorities. Incorrect data can involve data that is out of date or has been manipulated, for instance by failing to register complaints by citizens in order to make official crime statistics look better (Eterno & Silverman, 2012).

At the core of the protection of rights in criminal prosecution is the principle that citizens should be protected against both forms of contamination in the datasets of investigative authorities. This follows from the objectives of criminal proceedings, which state that all government intervention from the first police action must be legitimate. The public value of security in fact also entails the citizen's right to be protected against government intervention, and against random or illegitimate action during investigation. In my work with jurist Abhijit Das I have shown that – in theory – there are two filters for keeping dirty

data out of data-driven analyses: at the front-end and at the back-end of the process. At the front-end, this might mean the duty of police officers responsible for processing the information – privacy officials, policy workers or data professionals – of identifying dirty data and removing it from the datasets to be used. At the back-end of the process, it might be down to the judge to decide that the investigative authorities have obtained the data illegitimately or have used erroneous data. Examining the question of whether the use of both filters is actually sufficient to keep dirty data out of the government's datasets, we are forced to conclude that they are 'insufficiently transparent and fine-grained to offer effective protection against dirty data' (Das & Schuilenburg, 2020: 264). There is therefore a real risk that dirty data will make its way into analyses. This brings me to *throughput*, the processing of the data by algorithms.

b. Throughput

I previously showed that algorithms are increasingly used to support routine police activities and knowledge-intensive investigative tasks. The latter case might involve the processing of data for the purposes of criminal prosecution. In the current Dutch legal framework there is a tension between two key laws: the Police Data Act and the Code of Criminal Procedure. As various authors suggest, that tension can in part be traced back to the difference in the manner of standardisation between the two laws (e.g., Commissie Koops, 2018; Fedorova et al., 2022; Hirsch Ballin & Oerlemans, 2023). In contrast with the Code of Criminal Procedure, which primarily regulates the 'collec-

tion' of data, the Police Data Act offers a more general framework when it comes to the standardisation of its 'processing'. The supervisory task is also differently allocated in the two laws. In the Code of Criminal Procedure, the judge and the public prosecution service play a major supervisory role, while in the Police Data Act the main supervisory duties are allocated internally to police privacy officials and externally to the Dutch Data Protection Authority. In the context of the Protection Authority's supervision of compliance with the law it should be noted that its authority is very limited. For instance, it has no authority to stop the processing of data (Stevens et al., 2021).

In the literature, different legal issues have been identified in connection with the tension between the two laws. I will illustrate two issues with respect to the processing of data in a criminal prosecution context. One focal point is that the activities of collecting and processing data are in practice awkward to separate, as in the case of the authority to access a data carrier, which requires all kinds of processing operations to make the data usable for the investigation of crimes. Jurist Masha Fedorova and colleagues (2022: 157-158) point in this context to the implications of a separate standardisation. They note that the Police Data Act – which only regulates data collection – is primarily intended to ensure careful handling of data and not to standardise investigation, which is the job of the Code of Criminal Procedure. Another focal point is the fact that the intelligence function of the police, making information action-oriented by linking it with what is already known for the benefit of new criminal investigations, plays an important role besides the purpose of evidence collection and is becoming

increasingly interwoven with investigatory practice. The police's intelligence task, however, is not standardised in the Code of Criminal Procedure, but has its legal basis in the Police Data Act. Jurists Marianne Hirsch Ballin and Jan-Jaap Oerlemans (2023) therefore argue for a choice either for the standardisation of data-analyses in the Code of Criminal Procedure, or for a more detailed standardisation of analysis authorities in the Police Data Act.

c. *Output*

The process of collecting, storing and processing data ultimately leads to a concrete decision or recommendation of one or more actions within the framework of criminal proceedings, focused on the offender, the victim or the criminal infrastructure (*output*). The Committee on Modernization of Investigation in the Digital Age (known in Dutch as the 'Commissie Koops') points out that this process 'brings with it particular risks for the constitutional rights of citizens and the integrity of the investigation, such as the possible consequences of false positives and unfounded assumptions based on opaque algorithmic analyses' (2018: 26). For this reason, the Committee states that it would be desirable for the Code of Criminal Procedure to explicitly require automated data analyses and decision-making to be explicable.[5] Decisions in criminal proceedings must of course always be explicable, in the sense of being justified, but here the Committee means that in the case of decisions based on automated data analyses there is a risk of 'decisions that are not specifically justified, and thereby diffi-

cult to refute: "system says so"' (2018: 28). The importance of this extends to other areas besides decisions or actions in the context of police investigations. It applies also to decisions by the judge on such matters as granting prison leave or ending an order imposed on an offender, where the decisions are taken with the aid of risk assessment tools.

4.3 At the front-end of the problem

The legal standardisation of big data and algorithms should preferably be a forward-looking operation. By this I mean that technological developments move so rapidly and are driven by such turbulence that legislative frameworks should not only focus on what is needed today, but also anticipate the kind of effect AI will have on crime, and on investigation in particular, in the years to come. However, this is far from simple. Making laws and regulations suitable for today and the future is an extremely complex matter and an almost impossible task, as developments in AI come so thick and fast it is hard to get a grip on them. A familiar problem with new technology is that the outcome is uncertain and risks are difficult to estimate in advance. Legislation and regulation lag behind practice by definition, which means that before a law is introduced, the problems and risks have already changed. That's why I argue for developing new technology in such a way that the design and development phase takes into account what we consider important as a society – in this case, our public values. Four ethical schools of thought can be distinguished that make it possible to reflect on how moral considerations can be taken

into account in the design and development phases of technology (e.g., Van de Poel & Royakkers, 2011; Steen, 2023).

In consequentialism, the expected or foreseeable consequences of a technology determine whether it's deemed good or bad. This approach is substantially influenced by the utilitarian ideas of Jeremy Bentham, which consider positive consequences for use across the entire society most relevant. Bentham starts out from a rationalist view of humans and attempts to maximise the positive consequences of technology and minimise negative consequences by picking the option with the most or greatest advantages, and the fewest or smallest disadvantages. Deontology focuses not on the consequences of a technology but takes the principle as a starting point that should apply at all times, for example the right to privacy. Virtue ethics starts out from the question of what is a good way of living, emphasising among other things techno-moral virtues that are important in the design and development phase, such as the virtue of modesty, which can result in technology being developed in such a way that the human dimension prevails.

Relational ethics, the fourth school of thought, is based on the assumption that technology is embedded in a whole tangle of complex networks, which necessitates distancing ourselves from traditional dichotomies such as 'social vs technological' or 'human vs nature'. In this perspective, aspects such as justice and harm play an important role, and such matters cannot be separated from the fact that technology and our existence are completely intertwined. In other words, relational ethics is not a matter for humans alone, and its practical implications are

far-reaching. This means, for instance, that attention should also be paid to environmental harm from AI, as in the case of energy-guzzling data centres and the mountain of chemical waste created extracting the semiconductor materials indium and cobalt in African countries for touch screens and smartphone batteries (Crawford, 2021). I do not have exact figures, but the ecological footprint of our digital society – from smart household products to block chains and online meetings – makes up as much as 4% of total worldwide greenhouse gas emissions. Training self-learning algorithms also takes up countless hours of computer power.

Value sensitive design, which was put on the map by Batya Friedman and colleagues at the University of Washington (Friedman & Kahn, 2003), offers a framework for applying relational ethics in designing and developing new technology.[6] Technical, legal and ethical questions are examined together here with the aim of integrating driving, underpinning and procedural principles systematically into the design process. The underlying idea is that technology is not a neutral tool and that from the outset of initial development, people should consider its desirable and undesirable effects. An important point in value sensitive design is deciding which public values should be integrated into the design process and how this can be technically achieved. Friedman and her colleagues originally came up with a list of thirteen public values for information systems: 'human welfare, ownership and property, privacy, freedom from bias, universal usability, trust, autonomy, informed consent, accountability, courtesy, identity, calmness, and environmental sustainability' (Friedman, Kahn & Borning, 2006: 366).

Meanwhile, in *Ethics Guidelines for Trustworthy AI* (2019), the European Commission's High-Level Expert Group on AI has explicitly named the following four principles for AI systems: 'respect for human autonomy', 'prevention of harm', 'fairness' and 'explicability'. It will be clear that these principles also become increasingly important for government organisations in developing and using new AI applications.

4.4 Focal points

I mentioned above that gradually, using both legal rationale and ethical methodologies such as value sensitive design, attempts are being made to place digitalisation and algorithmisation of criminal investigation and law enforcement on the right track. In doing so, we should constantly keep an eye on how the distinction between driving values (such as security), underpinning values (privacy and non-discrimination) and procedural values (transparency) relate to one another. In striving to take more public responsibility for this, I would like to formulate a few critical focal points. These points relate to the following subjects: (a) defining and operationalising public values and (b) a plea for human intervention. I have noticed that these two topics are not clearly set out in the literature on AI.

a. Defining and operationalising

The first focal point is the tendency in methodologies such as value sensitive design to formulate what I will call meta-values.

It is unclear what exactly these entail and how they should be operationalised in a concrete AI application. An example might be the idea that algorithms should be transparent and explicable. These are well-known procedural principles and almost everyone acknowledges their importance. No one is going to argue against public organisations placing greater emphasis on these values in designing and deploying AI applications than has so far been the case. Transparency facilitates accountability for decisions taken by government organisations and the logic behind them, and it can help in improving algorithms by identifying possible errors ('debugging'). Nevertheless, defining and applying such public values in investigative practice is far from simple, partly due to the specific context and associated set of ethics in which algorithms are used. This is the question of defining and operationalising, an issue that has not been made sufficiently concrete in methodologies such as value sensitive design.

Take the public value of transparency in designing a new AI application to tackle crime. In practice, it will often prove difficult to answer the call for transparency in algorithms in a tangible way, such as by publishing and subsequently explaining the algorithm's black box. This is not only to do with the fact that making a process transparent doesn't directly make it explainable, or, as the Netherlands Scientific Council for Government Policy (WRR) states in *Mission AI*: 'Knowledge is not the same as understanding' (2023: 75). It also has to do with the fact that public values aren't ready-made principles, and that their significance and scope are always the subject of negotiation and conflict of interest between other parties such as data

professionals and policy makers. This makes the case for more empirical research into *how* values are brought to bear in the design of an AI application and are renegotiated in the realities of everyday life (cf. Latour, 1987; 1999; Carroll, 2021). For instance, there are often multiple values at stake which may conflict with each other while forming part of the day-to-day organisation of the system in which algorithms are applied. The added value of transparency will therefore need weighing up against other principles such as efficacy and privacy if algorithms are to be used for specific purposes. At the same time, the trade-off between values cannot be seen in isolation from the organisational practice around the use of algorithms. All this ultimately makes weighing up and selecting conflicting values within an organisation a decision with an inevitably 'political' quality, yet without any provision for democratic accountability.

When it comes to the actual possibilities and impossibilities of transparency, the discussion will not raise many questions in cases such as digital tools employed by educational institutions to investigate fraudulent use of ChatGPT in student assignments. But when it comes to a new and controversial investigative method such as the use of commercial DNA databases belonging to American companies to solve stalled murder cases in European countries, the matter is rather more complicated. Then the question is whether such a radical decision can be left to data professionals and policy makers in the police and the public prosecution service, or whether it wouldn't be better to hold an open parliamentary debate on the subject. What makes matters even more complicated is the increasing degree

to which data and algorithms are part of network-like chains between parties, in which data is shared and its use changes in meaning depending on the context as in the case of sharing images from Amazon's Ring doorbell with the police. Responsibility for the security and management of the images then lies with multiple parties, and the weighing up of conflicting values is no longer done in one place.

The fact that the organisational embedding of technology and the public values at stake cannot be viewed separately has far-reaching consequences. It means that transparency of the algorithm itself is an important public value, but an insufficient condition for responsible use of AI within an organisation – besides internal mechanisms, there is also a need for control and oversight of the effects of algorithms used by external parties (Meijer & Grimmelikhuijsen, 2021). Other authors go a step further by claiming that use of AI leads to so many ethical, legal and technical implications – from the *input*, *throughput* and *output* – that we have to question whether this can ever be managed responsibly in the government sector (Busuioc, 2021). Torin Monahan even believes that we should put a complete stop to the smokescreen of ethical principles in the development and deployment of big data applications. 'The only *ethical* surveillance is no surveillance,' Monahan (2023) writes in 'On the Impossibility of Ethical Surveillance'. This stance strikes me as impracticable, but it points to the problem of 'ethics-washing', where public and private parties primarily focus on maintaining the appearance of working in a socially responsible manner (Wagner, 2018).[7] Ultimately, ethics still remains a voluntary activity; you can opt in or out. This means

that an ethical approach to technology needs teeth – and there, again, the law is required.

b. Human in the loop

The second focal point I would like to mention is the broad call for accountability for AI decisions always to lie ultimately with people of flesh and blood. This is the issue of keeping a 'human in the loop', where someone possesses the knowledge, skill and resources to correct a wrong algorithmic decision.[8] In the security domain, this topic arises in the discussion on automated sentencing, or robot sentencing, where judges in the larger and more complex cases are replaced by verdicts churned out digitally by a computer. The argument for human intervention does not seem to be a remarkable position and encounters little resistance, as by keeping humans in the loop, human customisation remains possible and there is an identifiable person who can be held responsible for decisions.

Here, too, a warning is nevertheless called for. It would be naïve to view the human test as the ultimate counterweight to the disinterested judgement of an automated system. Like the justified concerns over prejudices in technology that reflect inequalities and stereotypes existing in our society, it should not be forgotten that professionals, too, have unconscious prejudices that affect their actions and decisions in concrete situations. Behavioural scientists point to the tendency to attribute intentions to events ('intentionality bias') and the drive to seek and select information that supports existing beliefs, while paying

less attention to information that contradicts it ('confirmation bias'). This can lead to erroneous decisions. In other words, a bias remains a bias, even if the shortcomings of the technology require a human solution.

There is another poison in AI that I have not yet mentioned. Any form of organisation is ultimately always disciplinary, in the sense that the insights mentioned above of Max Weber (bureaucracy) and Michel Foucault (discipline) are also true of an algocratic form of governance in which the outcomes of an algorithm have become the rationalisation behind decision-making in public organisations. Even with trained specialists 'in the loop', professionals may in fact want to take refuge in algocracy, as there are countless possible reasons for accepting the results of algorithms and complying with what the computer proposes. Compliance offers a certain degree of protection and security to legitimise decisions. In public administration, this is spoken of as 'potential accountability', whereby accountability can be assigned retrospectively in the case of abuse or calamity by blaming the algorithmic models (Noordegraaf & Sterrenburg, 2009). I have written with Rik Peeters about the phenomenon of 'machine justice' (Peeters & Schuilenburg, 2018) and the paradox that self-learning algorithms create an impression of a decision-making process constantly in motion, while in fact potentially leading to digital rigidity – strict and disciplined compliance with the results.

4.5 Socio-technological imagination

Aside from legal standards, ethical methodologies and better oversight of the use of AI by the government, even more data and more advanced algorithms are never the solution to problems of a socio-cultural nature such as crime and antisocial behaviour. Crime is a very complex problem and the same goes for tackling it. We now know that employment, in particular, can act as a solution for problems with crime, but this is not the perspective that AI applications in the security domain focus on today. The same logic applies to attempts to train algorithms to be 'bias-free' so that they don't make erroneous or dangerous choices. There are good reasons for that and it's a valuable development, as no one wants algorithms to play into the hands of discrimination. At the same time however, there is a risk of discrimination being reduced to a technological problem requiring a technological solution. That's like using a sticking plaster – it conceals the fact that discrimination is a deeply rooted social problem and that without an even playing field the outcomes will always remain unequal. That's what Ruha Benjamin means in *Race After Technology* when she writes, 'Algorithmic neutrality reproduces algorithmically sustained discrimination' (2019: 145). For genuine healing, you also need to tackle the underlying disease – daily discrimination on the basis of gender, ethnic background, skin colour, religion and income. This demands that combatting human and algorithmic discrimination go hand in hand.

The reason I bring these issues to the fore is to illustrate that a technical and economic approach to AI does not sufficiently

do justice to the complexity of socio-cultural problems. You might say there's a need for a socio-technological re-imagining of AI. In other words, could things be different? David Lyon poses this question when he writes, 'What might happen if surveillance were guided by an ontology of peace rather than of violence, an ethic of care rather than control, an orientation to forgiveness rather than to suspicion?' (2001: 153). It's a question with countless answers, which all have in common that we can only break free from a technical and economic perspective on AI by *doing* things differently. In criminal justice, examples of applications that go beyond increased efficiency might include applications to support individual judges in their work by linking characteristic elements of previous cases and thereby contributing to consistency and certainty of justice for citizens. Another possible application might be analysis of digital criminal records to gain greater insight into policy and law enforcement by parties such as the public prosecution service (Prins & Roest, 2018).

It can be cautiously concluded that there appear to be opportunities to use AI applications for purposes other than control and coercion, but Lyon's question touches on a more fundamental point. It brings us to the terrain of positive criminology, in which attention is drawn to the fact that security encompasses more than just the politics of 'law and order' and its warlike vocabulary of fighting and combat ('war on drugs', 'war on terror'). On an existential level, security is connected with interpersonal relationships of trust and care. This is reflected in the etymology of the Dutch word for security, 'veiligheid'. The word 'veilig' ('safe') originally goes back to the Middle

Low German *velich* and Old Frisian *felig*. The two words not only cover being 'without danger', but also point to qualities such as 'loyal', 'reliable', 'friendly' and 'shelter' (Schuilenburg, 2021: ch. 4).[9] The primal feeling of being at home somewhere gives rise to a sense of security, just like your connection with the neighbourhood where you live, and being able to rely on sufficient social contacts. A positive understanding of security is also Rosamunde van Brakel's conclusion when she says that 'big data applications can be used to identify what areas in a city need more attention (areas where, for example, an increasing number of young people are more at risk of radicalizing) and identify what specific problems in that area need to be addressed' (2016: 130). In this case, the focus of an AI application is closer to the notion of surveillance as medicine, care for security by a local network of schools, social workers and police officials, who are all close to the citizens and don't limit their attention to crime alone but address a broad range of questions, needs and problems on a neighbourhood level.

In conclusion, we need to look critically at what AI can *do* in the security domain, which is to say, we should think about a different approach from the standard reaction of exclusively deploying surveillance technology to combat problems of crime and antisocial behaviour. How can AI applications generate ideas of goodness and what society ought to be? Surely it must be possible to design AI applications that reinforce security in a positive way? Surely it must be possible to use AI applications that focus on improving issues such as care and trust? In order to attempt to find a way forward with this, we need to create socio-technological imaginaries of AI: new ways of thinking

and tackling seemingly intractable problems. The potential of the imagination, of the broadening of what intelligent systems can do and their significance in security, brings me to the human factor in AI.

Interlude IV. AI Experiences

The Apple Watch screen states that my average heart rate over the last ten minutes of my cycling workout has been 94. It then tells me my power to weight ratio and how many calories I've burned. The heart rate sensor of the Apple Watch uses a method known as photoplethysmography to detect how much blood flows through my wrist, and calculates my heart rate on this basis. I'm not sure why, but few digital gadgets give me as much pleasure as the Apple Watch. I'm aware that the luxury gadget on my wrist sees and records everything, from the medicines I take and the oxygen level of my blood to messages I send on WhatsApp and my spending on Apple Pay, yet I don't have any negative associations of oppression or influence over my choices.[1] On the contrary, the result is a feeling of pleasure and even security – not of control or coercion.

The Slovenian philosopher Slavoj Žižek would call this intentional self-deception – the pleasure I experience due to the stimuli of the Apple Watch is in fact a way of keeping my attention for as long as possible, gaining even greater and more subtle control over me: exercise so many minutes per day, take

medicine twice a day, and so on. Žižek certainly has a point, but in my view that does not exclude the possibility that digital surveillance need not only be thought of in terms of control and coercion. That is far too limited a view on the multiplicity of what I call AI experiences that people have when they use surveillance technology or become the subject of it, from consumers to security professionals. The current discourse on digital surveillance, however, offers little or no space for this positive side, the pleasure, play and relaxation (flirting with the camera, for instance) that's also part of our experience of surveillance technology (see also: Haggerty, 2006; Albrechtslund, 2008; Bell, 2009). Here I agree with what Kirstie Ball writes in 'Exposure': 'To date, discussions of the surveillance society have assumed a limited range of positions for the subject under surveillance, reducing the experience of surveillance to one of oppression, coercion, ambivalence or ignorance' (2009: 640).

There is a great deal of talk about the technical side of AI, about the technology behind algorithms and the datasets that algorithms use, but remarkably little about the human factor of AI. But when humans and technology are essentially interwoven, we also need to look at the way in which people relate to AI applications in practice and the experiences that determine how they interpret their relationship with digital surveillance, including the resistance against surveillance.[2] 'We need care, not cameras,' proclaimed a sign belonging to students demonstrating against the installation of smart cameras with facial recognition in Dutch university buildings to register how many people were in the lecture theatres and libraries. The cameras could also recognise the gender and age of students, and even

see whether individuals were wearing face masks to protect themselves against coronavirus.

Research into AI experiences fits into a long sociological tradition of symbolic interactionism. Herbert Blumer developed a theoretical model of this phenomenon as far back as the 1930s. The core idea is that individuals act on the basis of the meaning things have for them and that such meaning arises from social interactions, which is why it is constantly subject to change. A recent illustration of this was the response to the robot dog 'Digidog' used by the NYPD in arrests and exerting force. The animal terrified people and led to a storm of protest and mass resistance, with angry New Yorkers comparing it to films and stories in which machines have taken over the world and everyone's privacy has disappeared. The robot dog was relieved of its duties, but plans are currently being drawn up to patrol the border between the United States and Mexico with robot dogs, conducting the perfect surveillance.

The example of the New York robot dog raises many questions about freedom and legitimacy. Clearly there is unease at advancing automation in police work, but at the same time many people struggle to pinpoint how the function of the robot dog actually differs from that of a 'real' police dog. Aside from philosophical questions as to the autonomy of things, the protest of citizens in New York also concerns the legitimacy of the police, which depends on citizens trusting that police action be engaged and fair. The robot dog has become a symbol of the dehumanisation of the police force and its developing ever heavier weapons and advanced technologies instead of making

meaningful contact with citizens in the street.[3] The question is therefore which methods can contribute to a reinforcement of normative and social legitimacy of police action. This might be public control through the law or closer collaboration between citizens and the police with the aim of making communal values visible. In the latter case, it is conceivable that other parties than just data professionals might be involved in the development of new digital applications in order to identify and correct unintentional negative effects before their actual introduction.

The realisation is dawning that in order to strengthen public acceptance of intelligence systems, a dialogue is needed with stakeholders and citizens as to the effects and values that play a role here. This goes back to relational ethics and methodologies such as the above-mentioned value sensitive design, which looks at the way relevant human rights and public values can be identified in the earliest possible stage of the design and development process and how they can be built into the technology. All this sounds complicated, and it is, but the underlying idea of early involvement of stakeholders and citizens is that digitalisation and algorithmisation threaten to shift the discretionary space from individual treatment of cases (administrative law) and demand for evidence (criminal law) towards developing new technology. The role of software developers, network designers, system developers and data professionals with very specific technical knowledge has gradually come to be ever greater and more influential. In this context, I speak of a 'coding elite' – a predominantly white, male and heterosexual group making important choices in technological design and development

processes, from datasets used for input to the advanced algorithms that process the data.[4] Not only is there a risk that the discretionary space of these data professionals might evade control and accountability, but also that they might act without awareness of their own privileged position and discriminatory practices in taking decisions or carrying out actions based on algorithmic applications. Once the algorithms have been designed, a conversation about the results becomes increasingly difficult.

This demands another rethinking of the ways in which surveillance can be made public. In other words, can the perspective from the lived experiences of AI be part of good and appropriate care for digital technology? Here the issue of epistemic inclusion comes into play, the involvement of different forms of knowledge in the design and development process for new technology. 'Episteme' is derived from the Greek verb *epístamai*, which means 'knowing well, mastering, be familiar'. For many practical jobs such as policing and medicine, experiential knowledge – arising from reflection on one's own experiences – is of fundamental importance. For instance, when it comes to the diagnosis of a patient, doctors sometimes act on a gut feeling that something is wrong without there being any concrete medical evidence. Police officers and private security staff also use their intuition on a daily basis, in examining security camera images in the control room or on the street in contact with residents.[5] This feeling belongs to their arsenal of tools to make a decision or choose a solution in specific situations.

Experiential knowledge is valuable because it can make clear how AI applications are perceived in practice in a security setting, with all the emotions and feelings that can play a role. Gary Marx writes: 'Surveillance technology is not simply applied; it is also experienced by subjects, agents and audiences who define, judge and have feelings about being watched or a watcher' (2016: 173). You could use the above-mentioned concept of *mētis*, developed by the American political scientist James Scott, which refers to locally and situationally determined experiential knowledge. This practical knowledge differs from the dominant forms of knowledge often assumed to be universally valid, such as the technical knowledge of data professionals as to how an algorithm works or academic knowledge as to the efficacy of AI in investigating and tackling crime and antisocial behaviour.

Experiential knowledge, also known as tacit knowledge, is present on the street and in organisations but is yet to be encoded in academic books, procedures or mathematical formulas. This form of knowledge is hard to digitalise and will always remain the blind spot of AI. It cannot be captured in bits and bytes or generalised into abstract rules because it is bound up with personal experiences and is context-specific. The fact that not all forms of knowledge can easily be digitalised is an important insight in an algorithmic society. It means, among other things, that in the design and development process we should also think about the input of groups other than data professionals on the functioning of new technology and its impact on their existence.

This is the issue of social inclusion. It's about involving different layers of society in the design and implementation of new technology, which will in part depend on the type of application and the purpose for which it is used. But from the perspective of transparency and proportionality it is conceivable to include as diverse a team as possible in terms of gender, age and background in the design of new AI applications for digital surveillance. This would give a voice to everyone not yet included or insufficiently included in this area, such as young people and minorities, while also building a better understanding of the factors that affect how such groups think about new technology, for instance the use of smart sensor applications in neighbourhoods for security and liveability (Pavone, Santiago & Degli-Esposti, 2015; Snijders et al., 2019; TNO, 2021).

However, social and epistemic inclusion are not without problems. How can experiential knowledge be made accessible and comprehensible? How do you gain a clear view of all parties involved? Are all voices equally important? What should you do when opinions differ as to the public values at play? How do you ensure that the contribution of those involved is taken seriously and avoid the sense arising that there is merely the appearance of participation with no actual impact, a phenomenon termed *internal exclusion* by the American political scientist Iris Young (2000)?[6] These are important questions to which there is no unequivocal answer. That does not change the fact that experimentation with both forms of inclusion can lead to ever more engaging examples and applicable lessons in the field of AI and digital surveillance.

5 Towards a Digital Criminology

5.1 Introduction

'The problem always has the solution it deserves,' writes Gilles Deleuze, meaning that a solution always arises within the parameters in which something is defined as a problem. Based on the latest developments, I have examined how digitalisation of surveillance increasingly coincides with AI, and in particular with big data and algorithms, which is reflected in an intensification of both the scope and the depth of surveillance. Compared with traditional surveillance, digital surveillance is deployed more broadly and penetrates deeper into private life, because citizens are now watched from all sides and by everyone. I have also pointed out that there's always a provisional quality to AI, and ultimately a certain ambivalence, in that it offers solutions while simultaneously creating problems. I have specifically focused on the phenomenon of big data policing, where both public and private parties work with large volumes of data, using algorithms to provide smart analysis with the aim of making society secure.

The digitalisation and algorithmisation of surveillance in general, and that of investigating and tackling crime and antisocial behaviour in particular, tends to invoke an image of a simple dichotomy which either places the assumed technical and economic benefits in the foreground or emphasises the risks of AI. Regrettably enough, the debate therefore often gets stuck in a discussion in which you can either be in favour of privacy, or of decisive and efficient action against crime. So far there has been far less attention for the nature of the new AI applications themselves, the way in which they are embedded in a specific organisation, and how they are used in practice: by whom and for what purpose exactly is the data collected, which big data applications are used, who is the data shared with, and how do algorithms contribute to greater security in a specific context? As a result, the discussion on AI in the security domain itself exhibits many of the traits of a 'black box', that is to say, too little account is taken of questions such as who is using AI and for what purpose, or the consequences and effects of all this on society.

It seems necessary to me to conduct the debate as to the present and future of AI and digital surveillance more broadly than is currently happening. As the way we go about it – how we conceptualise and evaluate the two issues – also determines the scope of the debate, I have chosen to approach AI as an ethical and political issue that has a major influence on society as a whole and the security domain in particular. I have done this under the title 'Making Surveillance Public', with the aim of turning the spotlight on the various forms of digital surveillance used in investigating and tackling crime and antisocial

behaviour. Furthermore, I believe that technical progress without consideration of public values increases inequality and can lead to loss of social legitimacy of government organisations such as the police and local authorities. I have mentioned a number of these public values, focusing on driving, underpinning and procedural values, while always keeping in mind that there is an inherent tension in weighing up these values when investigating and tackling crime and antisocial behaviour. For instance, non-discrimination, transparency and algorithmic accountability are important principles, but so are security, efficacy and efficiency. Discussions as to the relationship between instrumentality and protection of rights date back as far as the history of investigation itself, but what seems different now is that in the AI sector, we are seeing a shift in certain aspects that we have always associated with either instrumentality or protection of rights. A couple of examples would be the role of privacy and the rise of private tech parties in security.

5.2 Privacy and private tech parties

Over the last two decades, more criminological research has been conducted into the way in which public duties and responsibilities in the security domain are in part carried out by parties other than the government. The police have become surrounded by a motley crew of 'police-like', or 'light-blue', organisations with whom they collaborate in ever-changing security assemblages to combat crime and antisocial behaviour, from insurance companies and retail associations to private security companies (Schuilenburg, 2015). We can add to this

list tech companies such as Amazon, Google and Tesla, but their role and power is not yet at the heart of criminological interests. Nevertheless, it is clear that these companies see a lucrative future in data relating to crime and antisocial behaviour. They not only buy up many small companies that are active in this area, but also sell crucial services and digital tools to the police and local authorities to prevent or investigate crime. An example of this is tackling crime and antisocial behaviour in 'smart cities', which takes place in part through security applications made by IBM and Siemens, from monitoring by streetlights to prevent burglaries to smart cameras that detect aggressive behaviour before it takes place. This means we will need to think about what role we should allow such companies to play in security policy. To what extent is dependence on tech companies desirable and how does the government retain oversight and authority over the data and algorithms used?

With respect to the public value of privacy, it's worth taking a fresh look at the phenomenon of luxury surveillance as part of broader socio-technological developments, such as the pluralisation and digitalisation of the role of the police. Luxury surveillance products are voluntarily purchased by citizens with the aim of monitoring others and themselves. The purchase of these products involves substantial sums of money, meaning that they are not accessible to everyone. They are closely linked to an exclusive lifestyle for individuals to express their identity and status, enabling them to distinguish themselves from others. The target group for these expensive items is often young people with a high level of education and income, who see the possession of items such as Tesla cars as a status symbol

(Li et al., 2021; Eski & Schuilenburg, 2022). This group of consumers consciously give up privacy, in the sense of control over their data and protection against abuse by third parties, in exchange for better service and additional security functions. This doesn't mean that privacy is a thing of the past or that it should no longer be protected. It indicates that the notion of privacy is changing in the interaction with technology.[1] For instance, there are frequent warnings of a division in society in which the underclass invariably forms the object of surveillance. In the case of luxury surveillance however, it looks like it is in fact the wealthier classes who allow themselves to be monitored and are willing to trade in their privacy, and that the exchange of personal data for security is considered advantageous.

Questions as to the right to privacy and the pluralisation of the function of the police have been around for a long time, but the current developments in AI and digital surveillance demand more criminological attention. These questions, after all, are increasingly levelled at criminology as the social trends of digitalisation and algorithmisation become more intertwined with the research field of criminology. What theoretical imagination is required here and what methodological demands does this make on criminologists? I have shown that parties such as the police, the courts and the prison system are embracing more and more tools in this area, the use of which have consequences for police work and, in a broader context, also for criminal justice and its application.[2] Digitalisation and algorithmisation effectively bring together old and new. The nature of investigation and decision-making changes, different competencies are

required, the discretionary space shifts towards data professionals, regulations are expressed in code, new forms of AI-crime arise and different forms of public accountability are needed. I'm convinced that criminology will become increasingly remote from everyday reality if it fails to incorporate such developments into its theoretical and empirical research on AI and digital surveillance.

An examination of these developments can take place in various ways. Empirical analyses of the effects of AI applications have a role to play, as does the mapping of digital developments in conceptual frameworks, the results of which should be subject to public debate. This requires interdisciplinary and transdisciplinary research, while comparative insights from different countries broaden the perspective on digitalisation and algorithmisation of the security issue. Interdisciplinary research might involve collaboration with technical and philosophical disciplines to better elucidate the complexity of the digital problem. In transdisciplinary research, scientific insights are combined with practical insights to stimulate the implementation of solutions.

5.3 Research agenda

It's time to return to the questions formulated in chapter 1 and state how they can be explored. Within the paths sketched out above, the following closely connected key points can be identified for academic research into the role of digitalisation and algorithmisation in security.

Theoretical imagination

In 2008, Chris Anderson, then editor-in-chief of *Wired*, wrote in *The End of Theory* that theories were becoming superfluous because the arrival of big data means that anything can be calculated. Anderson observes, 'With enough data, the numbers speak for themselves.' In other words, ditch the theoretical models and replace them with objective calculating models. His provocative claim that numbers go beyond subjective value judgements and differences in interpretation rests on a narrow vision of the nature of facts in general and theory in particular.[3] The Latin word for fact – *factum* – is derived from the verb *facere*, which means 'to make'; so when we talk about a 'fact' in an ontological sense, something that really 'exists', it always implies that we ourselves have constructed reality. Bare facts therefore don't exist, they have been ideologically tinted in advance. In addition, underlying any social science theory is a conceptualisation via 'sensitising' concepts which make researchers receptive to phenomena that they would otherwise miss (Van Swaaningen & Schuilenburg, 2018). These linguistic concepts work as a toolbox and help in the interpretation of the findings. Without such concepts and without slowing down to ask critical, fundamental questions, it would be impossible to place the social developments of digitalisation and algorithmisation in a framework. New tools for criminological reasoning are therefore very much needed in order to better understand (Weber's *Verstehen*) the digital field and to make it possible to reduce and experience such abstractions as the 'surveillance society', including variants such as the 'transparent society' and 'algorithmic society'.

Luxury surveillance, algorithmic psychopower, coding elite and feudal security are a few of the theoretical concepts that I have introduced in this context. However different these concepts may be, they imply that AI is always the embodiment or effect of certain forms of power and knowledge. These concepts enable us to pose questions as to the use of AI applications and its knock-on effects in citizens' lives: What form of power are we talking about? How does that power work? Who profits from it? I have shown that foreign tech parties are increasingly becoming a significant power factor in security and are fulfilling an existential need for security for various population groups. The state power of these techno-political parties is increasing rapidly, and their algorithmic manner of operating is described as both 'parasitic' (Merrifield, 2014) and 'predatory' (Durand, 2020). The role of tech parties in security invokes the question of whether security can still be seen as a 'thick' public good, to which every citizen should have the same level of access and in which state involvement is an essential condition for the social distribution of security. In order to answer this, we need a better grasp of the digital security field.

Empirical research

Let's turn to the practical side. From an academic perspective, plenty is known about the efficacy of traditional investigative methods and strategies that the police can use to prevent and investigate crime. There is far less insight into the efficacy of digital tools. For instance, research into AI is characterised by a shortage of empirical case studies beyond a handful of

exceptions mentioned time and again by everyone, such as the varying results of predictive policing. It is important that more knowledge is acquired in this area as to whether AI applications deliver the intended results – or whether, despite all good intentions, they in fact have the opposite effect – because claims as to their efficiency and efficacy carry more weight when they can also be empirically supported. That is not yet the case, and without empirical research these remain claims of little or no significance.

More intensive and long-term studies are needed to establish what's really going on with the effects of big data technologies and the social interactions between the general public and parties specialised in this area. Suitable examples would be content analyses of internet sites and participant observations in the ethnographic tradition of Erving Goffman or through the constructivist lens of the actor-network theory of Bruno Latour. The use of AI is socio-culturally determined, and even when it comes to big data technologies it is ultimately about real people of flesh and blood. In my view, there is therefore a great need to carry out qualitative research – alongside quantitative forms of data collection – into the AI experiences of citizens and professionals in order to become better acquainted with the perspective and the meanings these people attach to digital methods of surveillance. This fits into making surveillance public, because phenomena such as big data policing exist by the grace of 'social sorting' (Lyon, 2003) – one of the risks of which is that real people are reduced to abstract profiles, fading into the background and disappearing from the picture. Focusing on AI experiences deals with a social need to give a voice

to everyone who is currently going unheard or is heard too little on the subject of surveillance, such as the silenced voices of weak, vulnerable or marginalised groups and the meanings they attach to surveillance of and in their lives. But I'm also thinking of experiential knowledge of practising professionals such as police officials and private security personnel.

Algorithms are just like people. Self-learning algorithms also develop over the course of their lives, that much is clear. They meet other algorithms, reproduce, attach meaning to events, influence our lives with their actions and deliver results. In other words, algorithms make a difference in the practice they are part of, sometimes raising the question of whether humans are still in control. From a socio-technological perspective in which human and non-human entities are closely intertwined, there is little reason not to also examine an algorithm's agency. And yet this seldom happens. The fact that the 'actorship' of algorithms is insufficiently recognised is neither coincidental nor arbitrary, but arises because historically, humans have been central to the explanatory frameworks of criminology and the starting point of empirical research. When people speak of 'actors', they generally mean humans. This anthropocentric view is a problem because digital technology is a crucial part of human society. Criminological research will therefore also have to focus on what is non-human. Technical knowledge can offer more insight into the use and the risks of algorithms, but I'm also thinking of research methods that deliver other forms of knowledge.[4] From a narrative criminological perspective, for instance, a format such as biography can be used to describe the life of a self-learning algorithm by delving very, very deeply

into its development. I can imagine that someday, a biography might be written with the title *Seeing Like an Algorithm*, in which relevant events and the most important phases in the life of a self-learning algorithm are described step by step to provide a personal window into its world.

Social debate

Finally, I come to the public role of the researcher. Many scientists working on AI and digital surveillance feel more comfortable engaging with the technical side of the story than talking about the direct relationship of AI with power structures and people's lived experiences. The discussion about AI is therefore largely restricted to the expertise and contribution of technicians, with little or no involvement from other disciplines, in particular social sciences. Criminology has barely managed to make a mark on the political debate and on policy with respect to the use of AI in tackling crime. That's remarkable because there are many legal and ethical sides to new surveillance technology, and social concerns as to privacy, the risk of bias and abuse of power are entirely legitimate. At the same time big data and algorithms are performative, in the sense that they actively shape the security domain they are part of. I believe that without the introduction of big data and algorithmic models, police and local authorities would never have embarked on certain extensive and far-reaching investigations. Claudia Aradau speaks of an '"AI common sense" which is increasingly sedimented in the government of people and things' (2023: 303). An example would be tackling petty crime

such as pickpocketing and shoplifting under the Dutch police programme 'Sensing' in Roermond through algorithmic surveillance. In other words, there appears to be a certain lack of moderation in investigating crime and antisocial behaviour, partly fuelled by the tendency to develop the technology first, then determine its purpose, and only afterwards establish a legal base. In that respect, there is a need for a form of criminology to take part in the public debate about current data cravings and technological urges in the field of security, particularly when its insights are painful and go against the grain of public and political opinions.

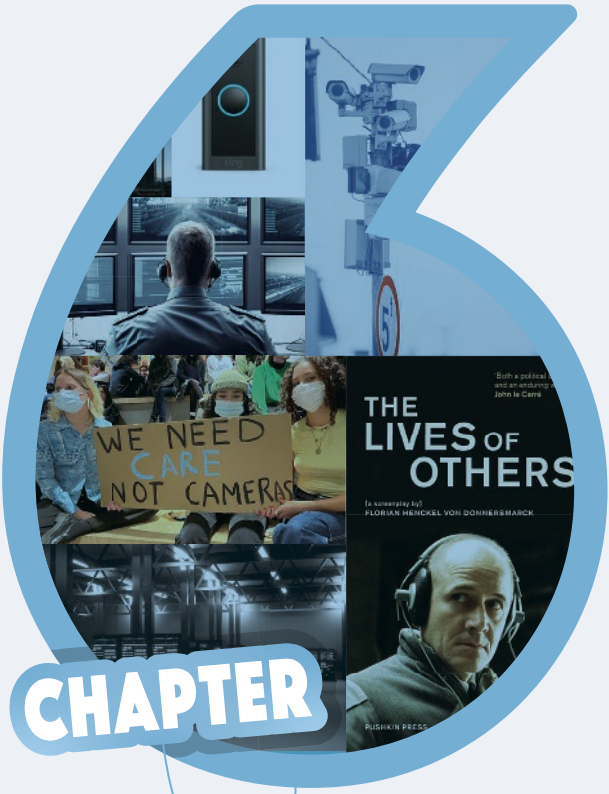
One of the ambitions of criminology is to produce knowledge through research, which is then shared with policy makers, the public and other parties. But criminological expertise can also be deployed in other ways. Progress in AI is moving so rapidly that it requires anticipation of its potential positive and negative effects on society. One way of dealing with this is to revise the position of criminology. It seems obvious, for instance, that academics should become involved earlier in the design of new AI applications, a position that comes close to what Ian Loader and Richard Sparks (2010) have termed an 'observer-turned-player'. It is in the design phase of AI applications that we can join data professionals and policy makers in thinking proactively and critically about the aims and values at play and how best to deal with them. What aim do people wish to achieve with AI? What values should be incorporated in its design? Of course, this position brings with it plenty of risks, balancing as it does between detachment and involvement. The danger of ethics-washing – where the scientist becomes part of

the 'system' and contributes to 'whitewashing' digital surveillance – always lurks in the background. I nevertheless believe that for criminology to fully embody its social responsibility, it must not wait until everything has been implemented before examining how it all works. To put it bluntly, that is too little, too late, because by then the key choices have already been made. Ergo, an extremely complex task for academics, but a role which, in my view, fits into what I have termed 'making surveillance public'.

5.4 Conclusion

The primary intention of this book was *not* to provide a blueprint for digital criminology, though something of an outline has come into view. In that regard, research into AI and digital surveillance also serves as an argument for digital criminology, a discipline focused on how the 'digital turn' is changing the playing field of criminology in terms of the nature, scale and of course backgrounds of crime. It doesn't stop there, however.[5] Digital criminology also addresses the effects of AI – directly or indirectly – in areas of forensic care, criminal justice and security practice: which digital tools are used and by whom, what results they lead to, and, no less importantly, against whom. For all this we need digital wisdom – which begins in education. In order for young people to be able to participate properly in society and to be able to carry out relevant research, the focus needs to be on teaching them digital skills, with colleges and universities promoting closer collaboration between criminology and technical and philosophical disciplines. It is the

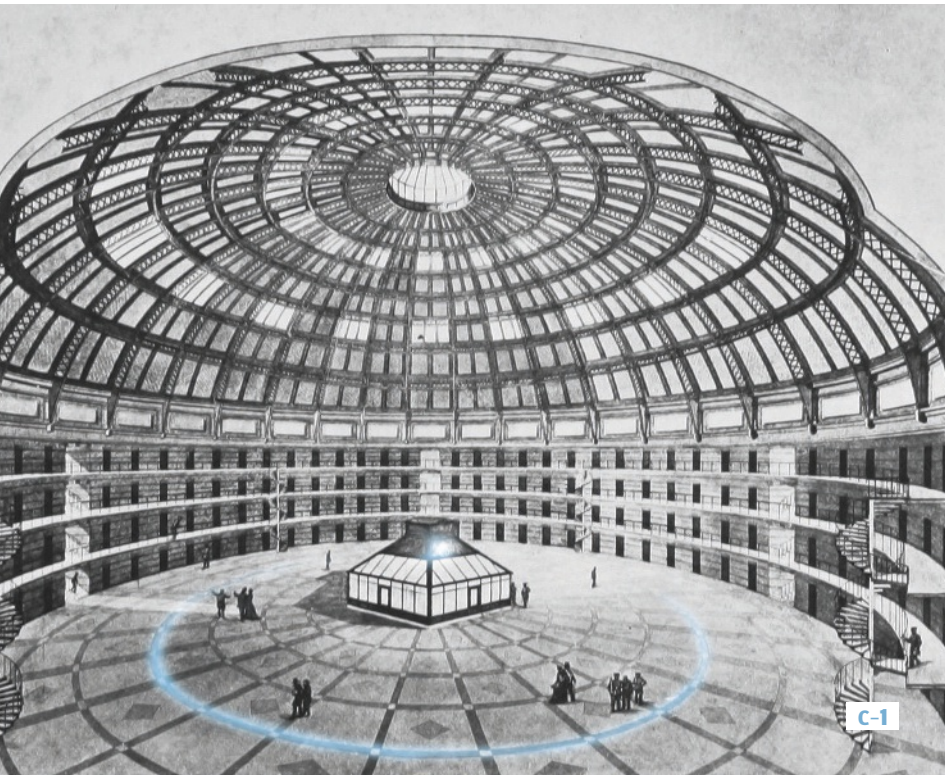
only way for us to better understand not only what AI can do, but also what AI is doing to us.


WE NEED
CARE
NOT CAMERAS
THE
LIVES OF
OTHERS
FLORIAN HENCKEL VON DONNERSMARCK
PUSHKIN PRESS
CHAPTER


ring


RECORDING
SENTRY ACTIVATED


164 Smith Street, Brooklyn, NY
spot the bubble
4:26
3 min
0.3 mi.




5t


DATA
DONATION

PANOPTICAR


DIGITALISATION
DATAFICATION
ALGORITHMISATION

MULTI SENSORY NORMALISATION

COMMODIFICATION

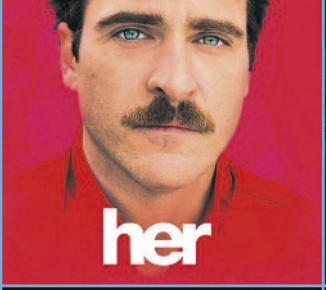

Avoid
Dangerous
Neighbourhood
18:22
22min
5km

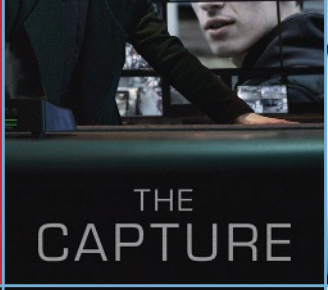
MOOD DETECTION

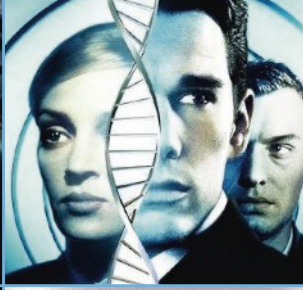

SCENT OF
ORANGES

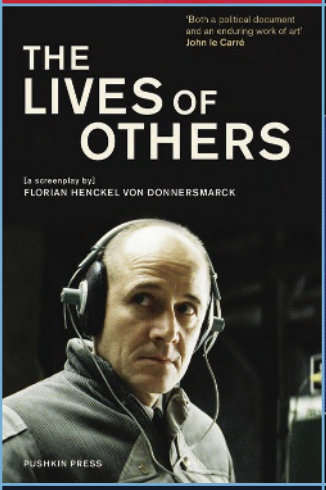
BY ABOVE BEYOND BELOW

BY ABOVE BEYOND BELOW


her

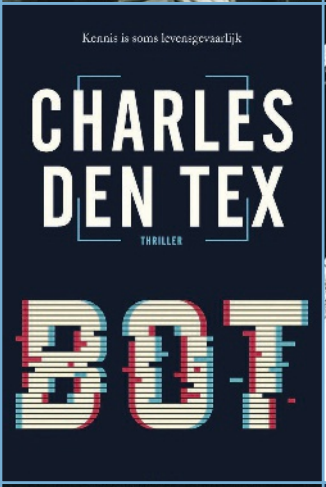

THE
CAPTURE



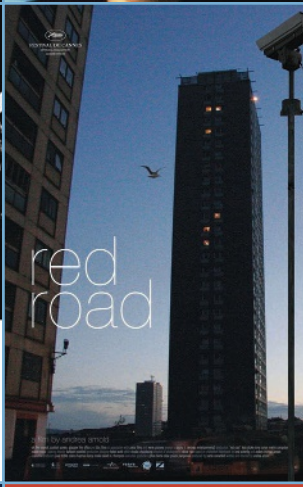

'Both a political document and an enduring work of art'
John le Carré
THE
LIVES OF
OTHERS
[a screenplay by]
FLORIAN HENCKEL VON DONNERSMARCK
PUSHKIN PRESS

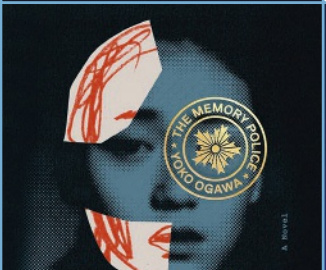

VIDEODROME
First it controls your mind
A SHOCKING NEW VISION
Then it destroys your body

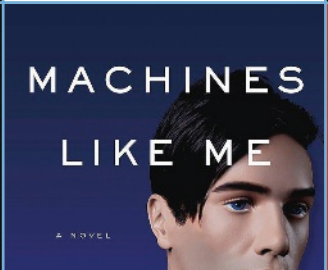

TIM ROBBINS SAMANTHA MORTON
a MICHAEL WINTERBOTTOM film
CODE 46

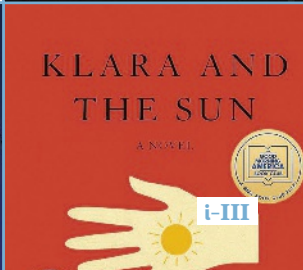

Kennis is soms levensgevaarlijk
CHARLES
DEN TEX
THRILLER
BOF

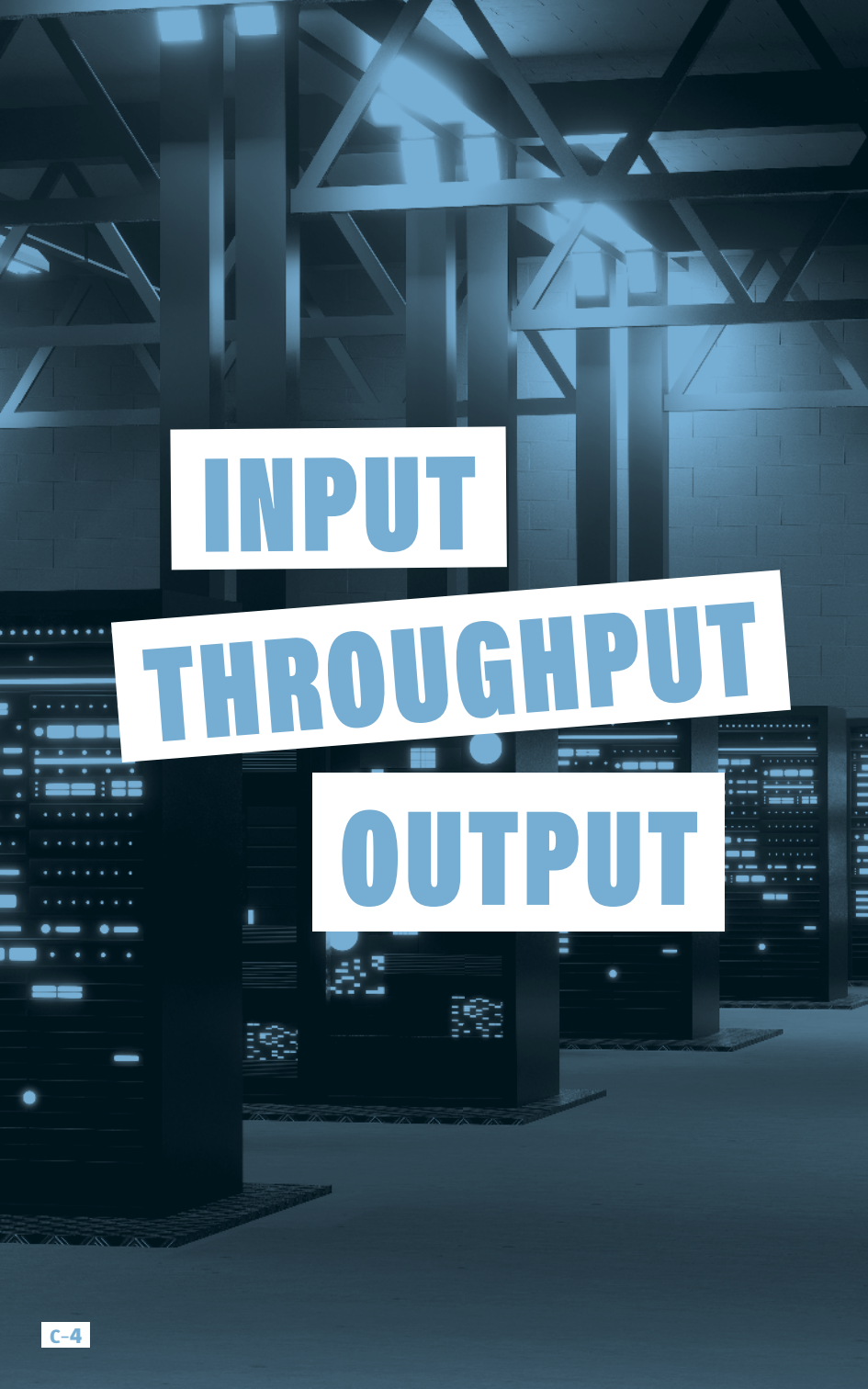

Visit the future where love is the ultimate crime.
THX 1138


red
road


THE MEMORY POLICE
YOKO OGAWA
A Novel

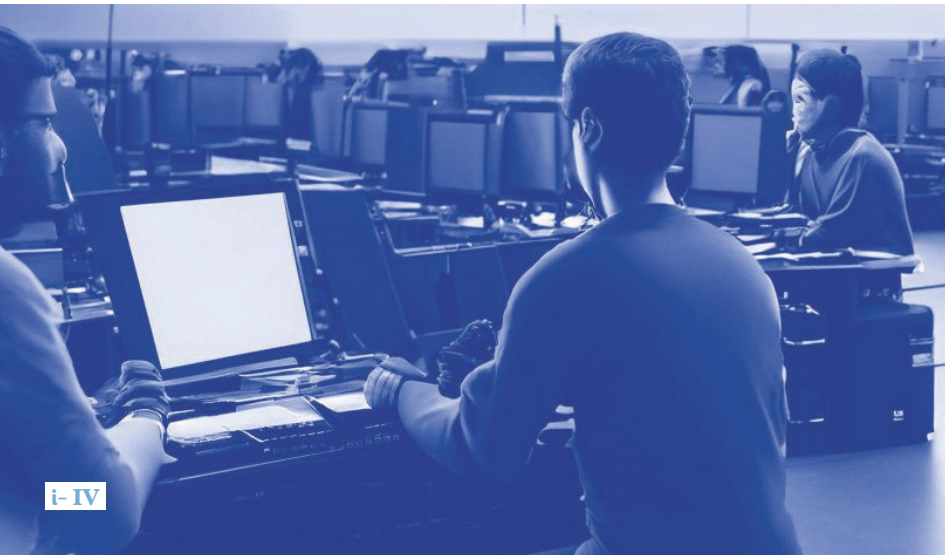

MACHINES
LIKE ME
A NOVEL


KLARA AND
THE SUN
A NOVEL


INPUT
THROUGHPUT
OUTPUT

DIRTY DATA

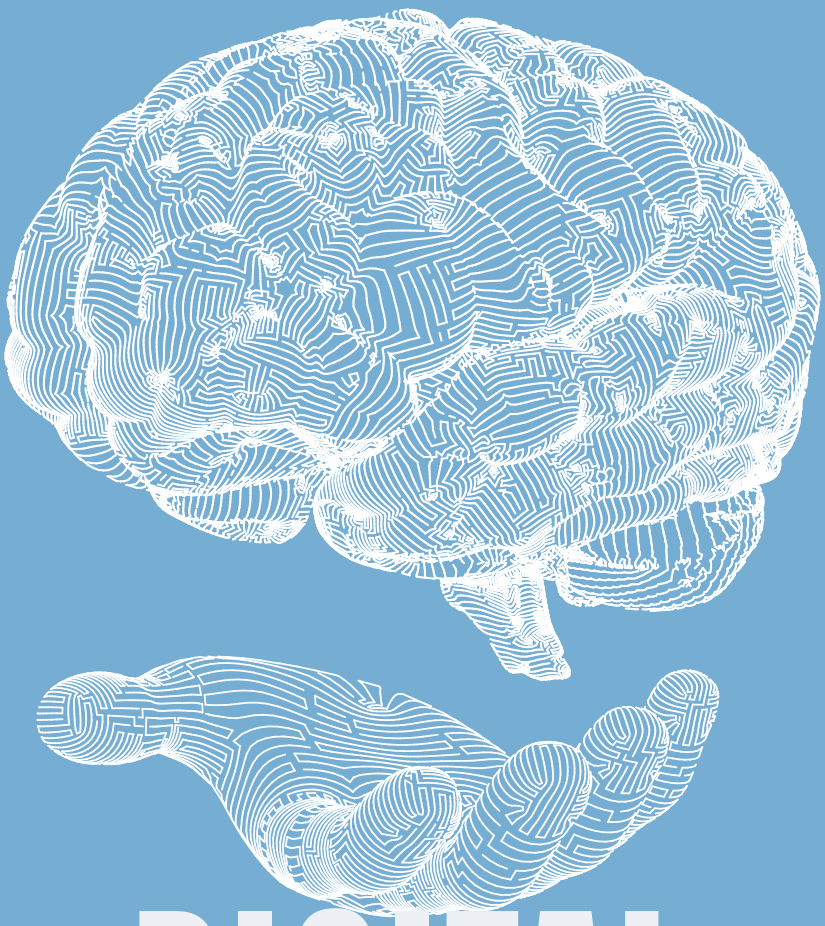

WE N
CAR
NOT




EED
RE
CAMERAS


CODING ELITE


X
X
X
X
X
X
X
X
X
X
X
X
X
X
X



DIGITAL SKILLS

Acknowledgements

This book could never have become what it is without the many conversations, discussions and collaborations with colleagues and friends. I began my research into digital surveillance more than seven years ago. Initially I focused primarily on predictive policing. Due to the rise of AI and algorithms, that research has since expanded substantially. My appointment as Professor of Digital Surveillance at Erasmus University Rotterdam has provided the occasion for writing this text, sketching out the background and themes of the research I intend to conduct with my research group over the coming years. I am most grateful to the Netherlands Organisation for Applied Scientific Research (TNO) and Erasmus University for making this position possible. I would like to mention three people who have read and provided rigorous comments on the text of this book: Rik Peeters, Richard Staring and Pieter Verrest. Another person I wish to mention here is Bob Hoogenboom: I'm grateful for your support and hope that we can expect good things to come. I would like to thank Onne Schuilenburg for the beautiful cover and attractive design. All credit for the translation of the text goes to Anna Asbury and Vivien Glass. I'm lucky to

have my family, Loes, Anna and Sara. Your cheerfulness and positivity are a gift in my life. This time, musical inspiration came from Autechre, Actress, Loraine James, Slowdive, Morrissey, Boards of Canada, The Necks and Don Cherry.

References

Albrechtslund, A. (2008), Online social networking as participatory surveillance, *First Monday*, 13(3), https://doi.org/10.5210/fm.v13i3.2142.

Amoore, L. (2011), Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times, *Theory, Culture & Society*, 28(6), 24-43.

Amoore, L. (2020), *Cloud Ethics. Algorithms and the Attributes of Ourselves and Others*, Durham and London: Duke University Press.

Anderson, C. (2008), The end of theory: The data deluge makes the scientific method obsolete, *Wired*, www.wired.com/2008/06/pb-theory.

Andrejevic, M. (2012), Ubiquitous surveillance, in: K. Ball, K. Haggerty & D. Lyon (eds.), *Routledge Handbook of Surveillance Studies* (pp. 91-98), New York: Routledge.

Andrejevic, M. & M. Burdon (2015), Defining the Sensor Society, *Television and New Media*, 16(1), 19-36.

Aneesh, A. (2006), *Virtual Migration: The Programming of Globalization*, Durham, NC: Duke University Press.

Aneesh, A. (2009), Global Labor: Algocratic Modes of Organization, *Sociological Theory*, 27(4), 347-370.

Aradau, C. (2023), Borders have always been artificial: Migration, data and AI, *International Migration*, 61, 303-306.

Arvidsson, A. (2010), Ethics and Value in Customer Co-production, *Marketing Theory*, 11(3), 261-278.

Ball, K. (2009), Exposure: Exploring the subject of surveillance, *Information, Communications and Society*, 12(5), 630-657.

Beer, D. (2009), Power through the algorithm? Participatory web cultures and the technological unconscious, *New Media & Society*, 11(6), 985-1002.

Beirne, P. (1987), Adolphe Quetelet and the Origins of Positivist Criminology, *American Journal of Sociology*, 92(5), 1140-1169.

Bell, D. (2009), Surveillance is sexy, *Surveillance & Society*, 6(3), 203-212.

Benjamin, R. (2019), *Race After Technology: Abolitionist Tools for the New Jim Code*, Medford, MA: Polity Press.

Blesse, S. & A. Diegman (2022), The place-based effects of police stations on crime: Evidence from station closures, *Journal of Public Economics*, 207, 1-19.

Boer, T. den & J.M. Harte (2023), Het recidiverisico in beeld en cijfers: De plaats en waarde van risicotaxatie-instrumenten in de weging van het recidiverisico, in: *Strafrechtelijke criminologie II. Een theoretische verdieping in de relatie tussen criminologie en strafrecht*, Willem Pompe Instituut: Boom Publishing.

Bogard, W. (2006), Surveillance Assemblages and Lines of Flight, in: D. Lyon (ed.), *Theorizing Surveillance* (pp. 111-136), Cullompton, Devon: Willan Publishing.

Borgers, M.J. (2007), *De vlucht naar voren*, The Hague: Boom.

Brabander, R. (2022), *Wees positief: Voorbij de retoriek van empowerment in het sociale domein*, Amsterdam: Amsterdam University Press.

Brayne, S. (2017), Big Data Surveillance: 'The Case of Policing', *American Sociological Review*, 82(5), 977-1008.

Brayne, S. (2021), *Predict and surveil. Data, discretion, and the future of policing*, New York: Oxford University Press.

Burrell, J. & M. Fourcade (2021), The Society of Algorithms, *Annual Review of Sociology*, 47(1), 213-237.

Busuioc, M. (2021), Accountable Artificial Intelligence: Holding Algorithms to Account, *Public Administration Review*, 81(5), 825-836.

Carraro, V. (2021), Grounding the digital: a comparison of Waze 'avoid dangerous areas' feature in Jerusalem, Rio de Janeiro and the US, *GeoJournal*, 86, 1121-1139.

Carroll, N. (2021), Augmented Intelligence: An Actor-Network Theory Perspective, *ECIS 2021 Research Papers*, June.

Castells, M. (1996), *The information age: Economy, society and culture, The rise of the network society, volume I*, Oxford: Blackwell Publishers.

Castells, M. (1997), *The information age: Economy, society and culture, The power of identity*, *volume II*, Oxford: Blackwell Publishers.

Castells, M. (1998), *The information age: Economy, society and culture, End of millennium*, *volume III*, Oxford: Blackwell Publishers.

CBS (2023), *Online veiligheid en criminaliteit 2022*, The Hague.

Clarke, R. (1988), Information technology and dataveillance, *Communications of the ACM*, 31(5), 498-512.

Clarke, R. (1994), The Digital Persona and its Application to Data Surveillance, *The Information Society*, 10(2), 77-92.

Commissie Koops (2018), *Regulering van opsporingsbevoegdheden in een digitale omgeving*, The Hague.

Crawford, K. (2021), *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, New Haven, CN: Yale University Press.

Cresswell, M. & H. Spandler (2009), Psychopolitics: Peter Sedgwick's legacy for mental health movements, *Social Theory & Health*, 7, 129-147.

Das, A. & M. Schuilenburg (2020), Garbage in, garbage out: Over predictive policing en vuile data, *Beleid en Maatschappij*, 47(3), 254-268.

Dean, J. (2022), Same As It Ever Was?, *New Left Review*, https://newleftreview.org/sidecar/posts/same-as-it-ever-was.

Deleuze, G. (1990), Post-scriptum sur les sociétés de controle, *L'Autre journal*, 3-7.

Derrida J. (1993), *Dissemination* (trans. B. Johnson), London: Athlone Press.

Dijk, G. van (2020), Algoritmische risicotaxatie van recidive. Over de Oxford Risk of Recidivism tool (OXREC), ongelijke behandeling en discriminatie in strafzaken, *Nederlands Juristenblad*, 95(25), 1784-1790.

Dixon, N. (2017), Stranger-ness and Belonging in a Neighbourhood WhatsApp Group, *Open Cultural Studies*, 1, 493-503.

Downey, A. (2023), *Neocolonial Visions: Algorithmic Violence and Unmanned Aerial Systems*, Aksioma: Ljubljana.

Durand, C. (2020), *Technoféodalisme: Critique de l'économie Numérique*, Paris: Zones.

Ericson, R.V. (2007), *Crime in an Insecure World*, Cambridge, UK: Polity Press.

Ericson, R. & K. Haggerty (1997), *Policing the Risk Society*, Toronto: University of Toronto Press.

Eski, Y. & M. Schuilenburg (2022), On Tesla: Balancing sustainable car connectivity, silent lethality and luxury surveillance, *Criminological Encounters*, 5(1), 234-251.

Eterno, J. & E. Silverman (2012), *The crime numbers game: Management by manipulation*, New York: Taylor & Francis Group.

Eysink Smeet, M., K. Schram, A. Elzinga & J. Zoutendijk (2019), *Alerte burgers, meer veiligheid? De werking van digitale buurtpreventie in Rotterdam*, Rotterdam: Hogeschool van Rotterdam.

Fedorova, M.I., R.M. te Molder, M.J. Dubelaar, S.M.A. Lestrade & T.F. Walree (2022), *Strafvorderlijke gegevensverwerking. Een verkennende studie naar de relevante gezichtspunten bij de normering van het verwerken van persoonsgegevens voor strafvorderlijke doeleinden*, Nijmegen: Radboud University Press.

Feeley, M. & J. Simon (1994), Actuarial Justice: The Emerging New Criminal Law, in: D. Nelken (ed.), *The Futures of Criminology* (pp. 173-201), London: Sage.

Ferguson, A.G. (2017), *The Rise of Big Data Policing. Surveillance, Race, and the Future of Law* Enforcement, New York: NUY-Press.

Flight, S. (2022), *Cameratoezicht door gemeenten: Evaluatie wetswijziging artikel 151c Gemeentewet*, Amsterdam.

Floridi, L. (2019), Translating Principles into Practices of Digital Ethics: Five Risks of Being Unethical, *Philosophy & Technology*, 32, 185-193.

Foucault. M. (1975), *Surveiller et Punir: Naissance de la prison*, Paris: Gallimard.

Foucault, M. (1976), *Histoire de la sexualite I: La volonte' de savoir*, Paris: Gallimard.

Foucault, M. (2004), *"Society Must Be Defended": Lectures at the Collège de France, 1975-1976*, London: Penguin.

Foucault, M. (2008), *The Birth of Biopolitics. Lectures at the Collège de France 1978-1979*, New York: Palgrave Macmillan.

Friedman, B. & P.H. Kahn (2003), Human Values, Ethics and Design, in: A. Jacko & A. Sears (eds.), *Handbook of Human-Computer Interaction: Fundamentals, Evolving Technologies, and Emerging Applications* (pp. 1177-1201), Mahwah, NJ: Lawrence Erlbaum.

Friedman, B., P.H. Kahn & A. Borning (2006), Value Sensitive Design and information systems, in: P. Zhang & D. Galetta (eds.), *Human-Computer Interaction and Management Information Systems: Foundations* (pp. 348-372), New York: M.E. Sharpe.

Fussey, P. & D. Murray (2019), *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, Colchester, Human Rights Centre: University of Essex.

Fussey, P. & A. Sandhu (2022), Surveillance arbitration in the era of digital policing, *Theoretical Criminology*, 26(1), 3-22.

Galič, M., A. Das & M. Schuilenburg (2023), AI and Administration of Criminal Justice. Report on The Netherlands, *e-Revue Internationale de Droit Pénal*, 5-61.

Galič, M., T. Timan & B.J. Koops (2017), Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation, *Philosophy and Technology*, 30, 9-27.

Galloway, A. (2021), *Uncomputable: Play and Politics in the Long Digital Age*, London: Verso.

Gandy, O. (1993), *The panoptic sort: A political economy of personal information*, Boulder, CO: Westview.

Garland, D. (2001), *The Culture of Control: Crime and Social Order in Contemporary Society*, Chicago: University of Chicago Press.

Gartner (2011), *Gartner Says Solving 'Big Data' Challenge Involves More Than Just Managing Volumes of Data*, www.gartner.com/it/page. jsp?id=1731916.

Giddens, A. (1984), *The Constitution of Society: Outline of the Theory of Structuration*, Cambridge, UK: Polity Press.

Giddens, A. (1990), *The Consequences of Modernity*, Cambridge, UK: Polity Press.

Gilliard, C. & D. Golombia (2021), Luxury Surveillance: People pay a premium for tracking technologies that get imposed unwillingly on others, *Real Life Magazine*, July.

Gilliom, J. & T. Monahan (2012), Everyday resistance, in: K. Ball, K. Haggerty & D. Lyon (eds.), *Routledge Handbook of Surveillance Studies* (pp. 405-412), Abingdon: Routledge.

Glaser, V.L., N. Pollock & L. D'Adderio (2021), The Biography of an algorithm: Performing algorithmic technologies in organizations, *Organization Theory*, 2(2), https://doi.org/10.1177/2631787721100460.

Gouldner, A. (1960), The Norm of Reciprocity: A Preliminary Statement, *American Sociological Review*, 25(2), 161-178.

Graaf, B. de (2013), *Ecce homo: Herkenning en registratie in de geschiedenis en veiligheidsbeleid*, Universiteit Leiden.

Haggerty, K. (2006), Tear down the walls: on demolishing the panopticon, in: D. Lyon, (ed.), *Theorizing surveillance* (pp. 23-45), Portland, OR: Willan.

Haggerty, K. & R. Ericson (2000), The surveillant assemblage, *British Journal of Sociology*, 51(4), 605-622.

Haggerty, K. & R. Ericson (2006), The new politics of surveillance and visibility, in: K. Haggerty & R. Ericson (eds.), *The new politics of surveillance and visibility* (pp. 3-33), Toronto: University of Toronto Press.

Han, B.-C. (2017), *Psychopolitics: Neoliberalism and new technologies of power*, London: Verso.

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

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

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

Hardyns, W. & A. Rummens (2017), Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges, *European Journal on Criminal Policy and Research*, 24, 201-218.

Hausken, L. (2016), The Archival Promise of the Biometric Passport, in: I. Blom et al. (eds.), *Memory in Motion. Archives, Technology, and the Social* (pp. 257-284), Amsterdam: Amsterdam University Press.

Hayward, K.J. & M.M. Maas (2021), Artificial intelligence and crime: A primer for criminologists, *Crime, Media, Culture*, 17(2), 209-233.

High-Level Expert Group on Artificial Intelligence (2019), *Ethics guidelines for trustworthy AI*, Brussels: European Commission.

Hirsch Ballin, M.F.H. & J.J. Oerlemans (2023), Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijk optreden, *Delikt en Delinkwent*, 1(2), 18-38.

Hobbes, T. (2003 [1651]), *Leviathan*, Bristol: Thoemmes Continuum.

Hoek, D. & J. Stigter (2021), Europol: An Overwhelming Stream of Big Data, *Revue Internationale de Droit Pénal*, 92(2), 19-44.

Huxley, A. (1932), *Brave New World*, London: Chatto & Windus.

IBM (2013), *The Four V's of Big Data*, www.ibmbigdatahub.com/infographic/four-vs-big-data.

Joh, E. (2014), Policing by numbers: Big Data and the fourth amendment, *Washington Law Review*, 89(1), 35-68.

Jong, J. de (2016), *Dealing with Dysfunction: Innovative Problem Solving in the Public Sector*, Washington D.C.: Brookings.

Kienscherf, M. (2022), Surveillance Capital and Post-Fordist Accumulation: Towards a Critical Political Economy of Surveillance-for-Profit, *Surveillance & Society*, 20(1), 18-29.

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

Kitchin, R. (2014b), The real-time city? Big data and smart urbanism, *GeoJournal*, 79(1), 1-14.

Kitchin, R. & G. McArdle (2016), What makes big data, big data? Exploring the ontological characteristics of 26 datasets, *Big Data & Society*, 3(1), 1-10.

Koopman, C. (2019), *How We Became Our Data: A Genealogy of the Informational Person*, Chicago and London: The University of Chicago Press.

Koskela, H. (2011), Hijackers and Humble Servants: Individuals as Camwitnesses in Contemporary Control Work, *Theoretical Criminology*, 15(3), 269-282.

Kosta, E. (2022), Algorithmic state surveillance: Challenging the notion of agency in human rights, *Regulation & Governance*, 16(1), 212-224.

Kraft, O. (2018), *Sharpening the money-laundering risk picture: How data analytics can support financial intelligence, supervision and enforcement*, London: Royal United Services Institute for Defence and Security Studies (RUSI).

Landman, W. & S. Groothuis (2022), *Politiewerk op het web. Een verkennend onderzoek naar online gegevensvergaring door de politie*, The Hague: Sdu Uitgevers.

Laney, D. (2001), 3D data management: Controlling data volume, velocity and variety, *META Group Research Note*, 6.

Lash, S. (2007), Power after hegemony: Cultural studies in mutation?, *Theory, Culture & Society*, 24(3), 55-78.

Latour, B. (1987), *Science in Action. How to Follow Scientists and Engineers through Society*, Cambridge: Harvard University Press.

Latour, B. (1999), *Pandora's Hope. Essays on the Reality of Science Studies*, Cambridge: Harvard University Press.

Lazzarato, M. (1996), Immaterial Labour, in: M. Hardt & P. Virno (eds.), *Radical Thought in Italy: A Potential Politics* (pp. 133-147), Minneapolis, MI: University of Minnesota Press.

Leloup, P. (2023), De historisering van (digitale) surveillance: fotografie als middel van toezicht en controle (late 19e – vroege 20e eeuw), *Tijdschrift over Cultuur & Criminaliteit*, (13)2, 33-49.

Leszczynski, A. (2016), Speculative futures: Cities, data, and governance beyond smart urbanism, *Environment and Planning A: Economy and Space*, 48(9), 1691-1708.

Lévi-Strauss, C. (1969 [1949]), *The Elementary Structures of Kinship*, Boston: Beacon Press.

Levy, K. (2022), *Data Driven: Truckers, Technology, and the New Workplace Surveillance*, Princeton, NJ: Princeton University Press.

Li, Y., J. Lin & S. Xu (2021), *Analysis of Tesla's Business Model: A Comparison with Toyota*, 2021 International Conference on Financial Management and Economic Transition (FMET 2021), Guangzhou, China.

Ligthart, S., D. van Toor, T. Kooijmans, T. Douglas & G. Meynen (2021), *Neurolaw: Advances in Neuroscience, Justice & Security*, Cham, Switzerland: Palgrave MacMillan.

Loader, I. & R. Sparks (2010), *Public Criminology?*, London: Routledge.

Lyon, D. (2001), *Surveillance Society: Monitoring Everyday Life*, Buckingham: Open University Press.

Lyon, D. (2003), *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*, London: Routledge.

Lyon, D. (2007), *Surveillance Studies: An Overview*, Cambridge: Polity Press.

Lyon, D. (2015), *Surveillance After Snowden*, Cambridge, UK: Polity Press.

Lyon, D. (2018), *The Culture of Surveillance*, Cambridge, MA: Polity Press.

Maalsen, S. & J. Sadowski (2019), The Smart Home on FIRE: Amplifying and Accelerating Domestic Surveillance, *Surveillance and Society*, 17(1/2), 118-124.

Maas, M., E. Legters & S. Fazel (2020), Professional en risicotaxatie-instrument hand in hand, *Nederlands Juristenblad*, 95(28), 2055-2060.

Mali, B., C. Bronkhorst-Giesen & M. den Hengst (2017), *Predictive policing: lessen voor de toekomst. Een evaluatie van de landelijke pilot*, Apeldoorn: Politieacademie.

Mann, S., Nolan J. & B. Wellman (2003), Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments, *Surveillance & Society*, 1(3), 331-355.

Manning, P. (2008), *The Technology of Policing: Crime Mapping, Information Technology, and the Rationality of Crime Control*, New York: New York University Press.

Marx, G.T. (2002), What's new about the "new surveillance"? Classifying for change and continuity, *Surveillance & Society*, 1(1), 9-29.

Marx, G.T. (2016), *Windows into the soul, Surveillance and society in an age of high technology*, Chicago: University of Chicago Press.

Mathiesen, T. (1997), The Viewer Society: Michel Foucault's 'Panopticon' Revisited, *Theoretical Criminology*, 1(2), 215-234.

Mauss, M. (2002 [1923-1924]), *The Gift: The Form and Reason for Exchange in Archaic Societies*, London: Routledge.

Mayer-Schönberger, V. & K. Cukier (2013), *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, London: John Murray.

McCahill, M. (2002), *The Surveillance Web: The Rise of Visual Surveillance in an English City*, Cullompton: Willan.

McGuire, M.R. & T.J. Holt (eds.) (2017), *The Routledge Handbook of Technology, Crime and Justice*, Abingdon: Routledge.

Meijer, A. & S. Grimmelikhuijsen (2021), Responsible and accountable algorithmization: How to generate citizen trust in governmental usage of algorithms, in: M. Schuilenburg & R. Peeters, *The Algorithmic Society: Technology, Power, and Knowledge* (pp. 53-66), London/New York: Routledge.

Meijer, A., S. Grimmelikhuijsen & M. Bovens (2021), De legitimiteit van algoritmisch bestuur: een systematisch overzicht van bedreigingen en oplossingsrichtingen, *Nederlands Juristenblad*, 96(18), 1471-1478.

Meijer, A. & M. Wessels (2019), Predictive Policing; Review of Benefits and Drawbacks, *International Journal of Public Administration*, 42, 1031-1039.

Memorie van toelichting bij het wetsvoorstel tot vaststelling van het Nieuwe Wetboek van Strafvordering (2020), The Hague.

Merrifield, A. (2014), The entrepreneur's new clothes, *Geografiska Annaler: Series B, Human Geography*, 96(4), 389-391.

Mohler, G.O., M.B. Short, S. Malinowski & M. Johnson (2016), Randomized Controlled Field Trials of Predictive Policing, *Journal of the American Statistical Association*, 110(512), 399-1411.

Mols A. & J. Pridmore (2019), When citizens are 'actually doing police work': The blurring boundaries in WhatsApp neighbourhood crime prevention groups in the Netherlands, *Surveillance & Society*, 17(3/4), 272-287.

Monahan, T. (2023), On the Impossibility of Ethical Surveillance, in: A. Pinchevski, P.M. Buzzanell & J. Hannan (eds.), *The Handbook of Communication Ethics*, New York: Routledge, *forthcoming*.

Morozov, E. (2013), *To save everything, click here*, New York: Public Affairs Books.

Morozov, E. (2022), Critique of Techo-Feudalism, *New Left Review*, 133-134.

Morrison, W. (1897), The interpretation of criminal statistics, *Journal of the Royal Statistical Society*, 60, 1-24.

Murphy, H. (2017), Algorithmic surveillance: The collection conundrum, *International Review of Law, Computers & Technology*, 31, 225-242.

Murray D. et al. (2023), The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe, *Journal of Human Rights Practice*, https://doi.org/10.1093/jhuman/huad020.

Neiva, L., G. Rafaela, & H. Machado (2022), Big Data applied to criminal investigations: expectations of professionals of police cooperation in the European Union, *Policing and Society*, doi: 10.1080/10439463.2022.2029433.

Noordegraaf, M. & J. Sterrenburg (2009), Publieke verantwoording en verantwoordingsdruk, in: M. Bovens & T. Schillemans (red.), *Handboek publieke verantwoording* (pp. 231-253), The Hague: Lemma.

Norris, C., J. Moran & G. Armstrong (1998), Algorithmic surveillance: The future of automatic visual surveillance, in: C. Norris, J. Moran & G. Armstrong (eds.), *Surveillance, Closed Circuit Television and Social Control* (pp. 255-276), Aldershot: Ashgate.

O'Neil, C. (2016), *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, London: Penguin Books.

O'Reilly, T. (2013), Open data and algorithmic regulation, in: B. Goldstein & L. Dyson (eds.), *Beyond Transparency: Open Data and the Future of Civic Innovation* (pp. 289-299), San Francisco, CA: Code for America Press.

Oerlemans, J-J. & W. van der Wagen (2021), Types of cybercrime and their criminalisation, in: W. van der Wagen, J.J. Oerlemans & M. Weulen Kranenbarg (eds.), *Essentials in cybercrime. A criminological overview for education and practice* (pp. 53-97), The Hague: Eleven International Publishing.

OESO (2013), *Exploring Data Driven Innovation as a New Source of Growth: Mapping the Issues Raised by "Big Data"*, www.oecd-ilibrary.org/science-and-technology/exploring-data-driven-innovation-as-a-new-source-of-growth_5k47zw3fcp43-en.

Orwell, G. (1984/2021), *Nineteen Eighty-Four*, Oxford: Oxford University Press.

Pali, B. & M. Schuilenburg (2020), Fear and Fantasy in the Smart City, *Critical Criminology: An International Journal*, (28)4, 775-788.

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

Pasquale, F. (2020), *New Laws of Robotics: Defending Human Expertise in the Age of AI*, Cambridge, MA: Harvard University Press.

Pavone, V., E. Santiago & S. Degli-Esposti (2015), *SurPRISE. Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe*, https://cordis.europa.eu/project/id/285492.

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

Peeters, R. & M. Schuilenburg (2023), Algorithmic Governance: Technology, Power, and Knowledge, in: W. Housley, A. Edwards, R. Beneito-Montagut & R. Fitzgerald (eds.), *The SAGE Handbook of Digital Society* (pp. 439-457), London: Sage.

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

Perry, W.L., B. McInnis, C.C. Price, S.C. Smith & J.S. Hollywood (2013), *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, Santa Monica: RAND Corporation.

Plato (1999), Phaedrus, *Verzameld Werk IV*, Kapellen: Pelckmans.

Powell, A., G. Stratton & R. Cameron (2018), *Digital Criminology*, London: Routledge.

Prins, C. & J. van der Rust (2017), AI en de rechtspraak: meer dan alleen de 'robotrechter', *Nederlands Juristenblad*, 93(4), 260-268.

Raad voor Strafrechtstoepassing en Jeugdbescherming (2021), *Advies: Risicotaxatie in de strafrechtstoepassing. Praktische, ethische en rechtspositionele aspecten belicht*, The Hague.

Rasch, M. (2020), *Frictie: Ethiek in tijden van dataïsme*, Amsterdam: De Bezige Bij.

Ratcliffe, J. (2014), What is the future of… predictive policing?, *Translational Criminology*, 6, 4-5.

Ratcliffe, J. (2016), *Intelligence Led Policing*, London: Routledge.

Ratcliffe, J.H., R.B. Taylor, A.P. Askey, K. Thomas, J. Grasso, K. Bethel, R. Fisher & J. Koehnlein (2021), The Philadelphia predictive policing experiment, *Journal of Experimental Criminology*, 17(1), 15-41.

Richardson, R., J. Schultz & K. Crawford (2019), Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice, *New York University Law Review Online*, 94(192), 192-233.

Ritzer, G. (1993), *The McDonaldization of Society: An Investigation into the Changing Character of Contemporary Social Life*, Thousand Oaks, CA: Pine Forge Press.

Rouvroy, A. & T. Berns (2013), Algorithmic governmentality and prospects of emancipation, *Réseaux*, 1, 163-196.

Rouvroy, A. & B. Stiegler (2016), The digital regime of truth: From the algorithmic governmentality to a new rule of law, *La Deleuziana: Online Journal of Philosophy*, 3, 6-29.

Sadowski, J., Y. Strengers & J. Kennedy (2021), More work for Big Mother: Revaluing care and control in smart homes, *Environment and Planning A: Economy and Space*, 0(0), https://doi.org/10.1177/0308518X211022366.

Schermer, B.W. (2022), *De gespannen relatie tussen privacy en cybercrime*, oratie, Leiden.

Schermer, B.W. & J.J. Oerlemans (2022), De EncroChat-jurisprudentie: teleurstelling voor advocaten, overwinning voor justitie?, *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 2, 82-89.

Schreurs, P. (2003), Emoties en bureaucratie. Kanttekeningen bij feministische kritiek op Webers uitspraken over emoties in de bureaucratie, *Tijdschrift voor Genderstudies*, 3, 33-44.

Schuilenburg, M. (2015), *The Securitization of Society: Crime, Risk, and Social Order*, New York: New York University Press.

Schuilenburg, M. (2021), *Hysteria: Crime, Media, and Politics*, London/New York: Routledge.

Schuilenburg, M. & R. Peeters (2017), Gift Politics: Exposure and Surveillance in the Anthropocene, *Crime, Law and Social Change*, (68)5, 563-578.

Schuilenburg, M. & R. Peeters (2018), Smart Cities and the Architecture of Security: Pastoral Power and the Scripted Design of Public Space, *City, Territory and Architecture*, 5(13), 1-9.

Schuilenburg, M. & M. Soudijn (2023), Big Data Policing: The Use of Big Data and Algorithms by the Netherlands Police, *Policing: A Journal of Policy and Practice*, 17, https://doi.org/10.1093/police/paad061.

Scott, J. (1998), *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*, New Haven & London: Yale University Press.

Sedgwick, P. (1982/2015), *Psycho Politics: Laing, Foucault, Goffman, Szasz and the Future of Mass Psychiatry*, London: Unkant.

Sekula, A. (1986), The Body and the Archive, *October*, 39, 3-64.

Sheptycki, J.W.E. (ed.) (2000), *Issues in Transnational Policing*, London & New York: Routledge.

Simon, J. (1987), The Emergence of a Risk Society: Insurance, Law, and the State, *Socialist Review*, 97, 61-89.

Simon, J. (1988), The Ideological Effects of Actuarial Practices, *Law and Society Review*, 22(4), 771-800.

Skatova, A. & J. Goulding (2019), Psychology of personal data donation, *Plos One*, 14(11), e0224240.

Slobogin, C. & S. Brayne (2022), Surveillance Technologies and Constitutional Law, *Annual Review of Criminology*, 6, 1-22.

Smith, G.J.D., L. Bennett Moses & J. Chan (2017), The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-driven Approach, *The British Journal of Criminology*, 57(2), 259-274.

Snaphaan, T. & W. Hardyns (2021), Handvatten voor een kwaliteitsbeoordeling van big data: De introductie van het Total Error raamwerk, *Tijdschrift voor Veiligheid*, (20)4, 63-88.

Snijders, D., M. Biesiot, G. Munnichs, R. van Est, met medewerking van S. van Ool en R. Akse (2019), *Burgers en sensoren – Acht spelregels voor de inzet van sensoren voor veiligheid en leefbaarheid*, The Hague: Rathenau Instituut.

Srnicek, N. (2017), *Platform Capitalism*, Cambridge: Polity Press.

Srnicek, N. (2012), Data, Compute, Labor, in: M. Graham & F. Ferrari (eds.), *Digital Work in the Planetary Market* (pp. 241-261), Cambridge, Massachusetts: The MIT Press.

Stalder, F. (2002), Privacy is not the Antidote to Surveillance, *Surveillance and Society*, 1(1), 120-124.

Staples, W.G. (2000), *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*, Lanham, MD: Rowman and Littlefield.

Steen, M. (2023), *Ethics for People Who Work in Tech*, Boca Raton, FL.: Chapman and Hall/CRC.

Steijns, M. (2021), *AI van repliek gediend: Een verkenning van tegenmacht vanuit maatschappelijke organisaties*, WRR Working Paper, 50, The Hague.

Stevens, L., M. Hirsch Ballin, M. Galič et al. (2021), Strafvorderlijke normering van preventief optreden op basis van datakoppeling, *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 4, 234-245.

Stickle, B. (2023), Crime Sharing: How the Sharing Economy May Impact Crime Victims, *Victims & Offenders*, doi: 10.1080/15564886.2022.2159905

Stiegler, B. (2006), Within the limits of capitalism, economizing means taking care, http://arsindustrialis.org/node/2922.

Stiegler, B. (2010), *Taking Care of Youth and the Generations*, Stanford: Stanford University Press.

Stiegler, B. (2011), *The Decadence of Industrial Democracies: Disbelief and Discredit, Volume I*, Cambridge: Polity Press.

Stiegler, B. (2012), Relational Ecology and the Digital Pharmakon, *Culture Machine*, 13, 1-19.

Stiegler, B. (2014), *The re-enchantment of the world. The value of spirit against industrial populism*, London: Bloomsbury.

Stoddart, E. (2011), *Theological Perspectives on a Surveillance Society: Watching and Being Watched*, Surray, UK: Ashgate.

Stoddart, E. (2021), *The Common Gaze: Surveillance and the Common Good*, London: SPCK.

Sunstein, C. (2014), *Why Nudge? The Politics of Libertarian Paternalism*, New Haven & London: Yale University Press.

Taylor, L. (2017), What is data justice? The case for connecting digital rights and freedoms globally, *Big Data & Society*, 4(2), 1-14.

Taylor, L., L. Floridi & B. Van der Sloot (eds.) (2017), *Group Privacy: New Challenges of Data Technologies*, Dordrecht: Springer.

Terpstra, J. (2010), *De maatschappelijke opdracht van de politie. Over identiteit en kernelementen van politiewerk*, Amsterdam: Boom Juridische uitgevers.

Terpstra, J. & R. Salet (2023), Het einde van PredPol: Het einde van predictive policing?, *Cahiers Politiestudies*, 66, 209-216.

Thaler, R.H. & C.R. Sunstein (2008), *Nudge: Improving Decisions About Health, Wealth, and Happiness*, New York: Penguin Books.

Tiqqun (2020 [2001]), *The Cybernetic Hypothesis* (trans. Robert Hurley), Los Angeles, CA: Semiotext[e].

TNO (2021), *Op zoek naar de mens in AI: Betrek de burger en experimenteer op verantwoorde wijze*, The Hague.

Trein, P. & F. Varone (2023), Citizens' agreement to share personal data for public policies: trust and issue importance, *Journal of European Public Policy*, doi: 10.1080/13501763.2023.2205434.

Van Brakel, R. (2016), Pre-emptive big data surveillance and its (dis) empowering consequences: the case of predictive policing, in: B. van der Sloot, D. Broeders & E. Schrijvers (eds.), *Exploring the boundaries of big data* (pp. 117-141), Amsterdam: AUP.

Van de Poel, I. & L. Royakkers (2011), *Ethics, Technology, and Engineering: An Introduction*, Chichester, U.K.: John Wiley and Sons.

Van de Sandt, E., A. van Bunningen, J. van Lenthe & J. Fokker (2021), *Towards Data Scientific Investigations: A Comprehensive Data Science Framework and Case Study for Investigating Organized Crime and Serving the Public Interest*, paper presented at the Third INTERPOL-UNICRI Global Meeting on AI for Law Enforcement, 25 November 2020, REPHRAIN.

Van Steden, R. & S. Mehlbaum (2021), Do-it-yourself surveillance: The practices and effects of WhatsApp Neighbourhood Crime Prevention groups, *Crime, Media, Culture*, 18(4), 543-560.

Van Swaaningen, R. & M. Schuilenburg (2018), Theoretische vernieuwing in de criminologie, *Tijdschrift over Cultuur & Criminaliteit*, (8)1, 3-18.

Van Tuinen, S. (2023), The Use of Souls: Souriau and Political Spirituality, *Aisthesis. Pratiche, Linguaggi E Saperi dell'estetico*, 15(2), 103-113.

United Nations (2021), *Racial and xenophobic discrimination and the use of digital technologies in border and immigration enforcement*, A/HRC/48/76, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/379/61/PDF/G2137961.pdf?OpenElement.

Wagner, B. (2018), Ethics as an Escape from Regulation: From "Ethics Washing" to Ethics Shopping?, in: E. Bayamlioğlu, I. Baraliuc, L. Janssens & M. Hildebrandt (eds.), *Being Profiled: Cogitas Ergo Sum* (pp. 84-88), Amsterdam: Amsterdam University Press.

Weber, M. (1958), *Essays in Sociology* (trans. and ed. by H.H. Gerth & C. Wright Mills), New York: Oxford University Press.

Weber, M. (1988), *Gesammelte Aufsätze zur Religionssoziologie I*, Tübingen: Mohr Siebeck.

Weber, M. (2006 [1921/1922]), *Wirtschaft und Gesellschaft*, Paderborn: Voltmedia GmbH.

Wessels, M. (2023), Accountability of Algorithmic Policing: Eight Sociotechnical Challenges, *Policing and Society*, doi: 10.1080/10439463.2023.2241965.

Whitman, M. (2020), "We called that a behavior": The making of institutional data, *Big Data & Society*, 7(1), 1-13.

Willems, D. & R. Doeleman (2014), Predictive Policing – wens of werkelijkheid?, *Tijdschrift voor de Politie*, 4/5, 39-42.

WRR (2011), *iGovernment*, Amsterdam: Amsterdam University Press.

WRR (2015), *The public core of the Internet: An international agenda for Internet governance*, Amsterdam: Amsterdam University Press.

WRR (2023), *Mission AI: The New System Technology*, The Hague: Springer.

Yeung, K. (2017), "Hypernudge": Big data as a mode of regulation by design, *Information, Communication & Society*, (20)1, 118-136.

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

Young, I.M. (2000), *Inclusion and Democracy*, Oxford: Oxford University Press.

Zedner, L. (2007), Pre-crime and post-criminology?, *Theoretical Criminology*, 11(2), 261-281.

Zuboff, S. (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, NY: Public Affairs.

Notes

Chapter 1

1 I restrict myself here to humans, but it should be noted that surveillance can also apply to animals, plants and objects.

2 Anthony Giddens (1990) terms surveillance the fourth institutional dimension linked with the modern age and rise of the nation state – following on after industrialism, a capitalist economy and military power. While military power is related to the control of the means of violence, surveillance involves monitoring of society and control of information.

3 In this connection, Michel Foucault adopts the neologism 'governmentality' ('gouvernementalité') in which the emphasis is on 'fostering life'. It is about the impact of a pastoral power that goes back to the pre-Christian Eastern world and is focused on offering care, in the sense that the welfare of everyone (*omnes*) and each person individually (*singulatim*) are central (Schuilenburg, 2015: 70-72).

4 Historically, the image of a sovereign power stems from the seventeenth-century British philosopher Thomas Hobbes (2003 [1651]) and his description of the Leviathan, the divine symbol of

a sovereign power who takes the form of the monarch, protecting his subjects against the fear of the other and the constant threat of violence.

5 For an overview of camera monitoring in the Netherlands, see: Flight (2022).

6 Further Vs have been added over the years, including *veracity* and *value* (IBM, 2013; OESO, 2013).

7 In this text I follow the definition of the High-Level Expert Group on Artificial Intelligence. Although the term 'AI' was coined as early as the 1950s in the military milieu, it is very difficult to give a uniform description of it. One of the problems is the use of the designation 'intelligence'. Its use would wrongly give the impression that machines do the same as humans. The term in this case refers to cognitive intelligence while humans in fact possess many more forms of intelligence, including emotional and social intelligence.

8 See: www.nrc.nl/nieuws/2022/09/01/met-microfoons-racisme-in-het-voetbal-bestrijden-a4140501 (visited: 22 August 2023).

9 Dutch research into the nature of policing and the associated use of surveillance only begins at the end of the 1990s and focuses largely on street monitoring by police officers (Terpstra, 2010).

10 Predictive policing is seen worldwide as the 'shining example, standard and icon of the police's new data-driven and prevention-focused approach' (Terpstra & Salet, 2023: 209). A telling feature of the euphoria in the Netherlands around its national deployment was the projection that the technology would allow the police to predict around 40% of burglaries and 60% of muggings (Willems & Doeleman, 2014).

Interlude I

1 See: https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/ (visited: 18 September 2023).

Chapter 2

1 The literature distinguishes between cybercrime in a narrow sense and computer-related offenses. Cybercrime refers to offenses in which the goal is computers and the data stored on them, as in the case of computer hacking. Computer-related crime refers to traditional misdemeanours that are committed (in part) with the aid of computers. There is also cyber-facilitated crime, in which digital technologies are used to facilitate the act (Oerlemans & Van der Wagen, 2021; Schermer, 2022).

2 Criminologists Keith Hayward and Matthijs Maas (2021) describe three categories how AI can be used for criminal activities: (1) crimes with AI (e.g., deepfakes and voice cloning), (2) crimes on AI (AI-hacks), and (3) crimes by AI (e.g., algorithmic market manipulation and price fixing).

3 In 2022, 15% of Dutch people aged 15 or older had been victims of one or more forms of cybercrime in the past year (CBS, 2023).

4 Research by ProPublica reveals that the actuarial tool COMPAS, used in the United States in deciding matters such as the level of penalties, systematically assigns higher recidivism scores to Afro-American individuals and individuals from other minority groups. See: www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm (visited: 26 August 2023).

5 Viktor Mayer-Schönberger and Kenneth Cukier define datafication as follows: 'to put a phenomenon in a quantified format so that it can be calculated and analysed' (2013: 78).

6 Other terms that regularly crop up in this context include 'digital persona' (Clarke, 1994), 'data shadow' (Stalder, 2002) and 'data derivative' (Amoore, 2011). A drawback of these terms is the suggestion they convey that people are passive objects, waiting to be classified and allocated by private companies and public organisations. This fails to recognise that individuals can also actively and voluntarily give away information, for instance to companies interested in personalized marketing or offering discounts for their products or services. This is data donation (discussed in Interlude I).

7 In 2020, The Hague District Court delivered a judgment concluding that the legislation regulating the use of SyRI did not strike a fair balance, as required under the European Convention on Human Rights (particularly in relation to the right to respect for private life in Article 8). According to the Dutch court, 'the application of SyRI is insufficiently transparent and verifiable. As such, the SyRI legislation is unlawful, because it violates higher law and, as a result, has been declared as having no binding effect' (Galič, Das & Schuilenburg, 2023).

8 It is often difficult to draw the boundary between automatic and autonomous weapons systems, a theme of particular relevance to warfare and the military rationale of pre-emption (Downey, 2023).

9 This applies to similar surveillance concepts, such as 'synoptic surveillance', where the public can look in on factory measuring equipment to check whether emissions of particular substances remain within legal limits.

10 It's worth noting that the term 'network' is used less and less frequently in the current literature and has been replaced by 'platform'. For instance the term barely comes up in the work of Shoshana Zuboff (2019) and Nick Srnicek (2017). The Spanish sociologist Manuel Castells is seen as the founder of the theory of the network society. In three weighty tomes published in the 1990s – *The Information Age* (1996; 1997; 1998) – he described how the economic, political and social structure of a society is determined and shaped to a significant extent by informational processes. Castells' work has been very influential in criminology when it comes to the perspective of 'nodal governance', developed by Clifford Shearing in collaboration with colleagues such as Les Johnston and Jennifer Wood (Schuilenburg, 2015).

11 Unlike internet investigation, OSINT has a non-criminal character and takes place on the basis of the police's general mission (in Dutch law, art. 3 Politiewet 2012). This leads to a great lack of legal clarity because in practice the boundary between intelligence and investigation is very diffuse (Landman & Groothuis, 2022).

12 The platform economy also offers alternatives to criminal law. Platforms such as Airbnb and Uber have their own form of conflict resolution and conflicts are solved before a judge gets a look-in (Stickle, 2023).

13 See: www.theguardian.com/lifeandstyle/2021/sep/23/the-smart-toilet-era-is-here-are-you-ready-to-share-your-analprint-with-big-tech (visited: 10 September 2023).

14 Another reason why the volume of datasets is becoming less relevant has to do with the definition of 'big'. What would have been seen as 'big' ten years ago would no longer be labelled that way now. There has also been an observable shift in emphasis from collecting data to designing, training and applying algorithms.

Authors such as Nick Srnicek (2022) expect these activities to become increasingly important, requiring more capital and expertise, which can lead to the risk of monopoly by tech companies.

15 Such aspects can also be traced back to the classic work *The McDonaldization of Society* by American sociologist George Ritzer (1993), in which he uses the example of the hamburger chain to show how contemporary society functions and the side-effects this can lead to. Nevertheless, there are other issues which also play a role in the decision as to whether a technological or other invasive innovation is adopted in an organisation. In the case of the police force, for example, Jan Terpstra and Renze Salet (2023) point to processes of imitation (isomorphism), involving examining other organisations that are seen as forerunners or pioneers of digitalisation processes.

16 Weber gives the following definition of bureaucracy: 'Bureaucracy develops the more perfectly, the more it is "dehumanized", the more completely it succeeds in eliminating from official business love, hatred, and all purely personal, irrational, and emotional elements which escape calculation' (1958: 8).

17 Concepts that are also used in this connection include 'algorithmic regulation' (O'Reilly, 2013; Yeung, 2017; 2018) and 'algorithmic governmentality' (Rouvroy & Berns, 2013; Rouvroy & Stiegler, 2016; Hannah-Moffat, 2019). For the differences between these approaches, see: Peeters & Schuilenburg (2023).

Interlude II

1 Peter Sedgwick, a Marxist and trained psychologist, is one of the first scholars to have used the term 'psychopolitics'. In *Psycho Politics* (1982), he criticises the conservative undercurrents in the work of philosophers who have dabbled in 'antipsychiatry', including Erving Goffman, Michel Foucault and Ronald Laing (see also: Cresswell & Spandler, 2009). A current contributor to the debate, the German-Korean philosopher Byung-Chul Han uses the term in *Psychopolitics* (2017) to show that the old forms of coercion have been replaced by neoliberal techniques for subjugation.

2 Without falling back into Cartesian mind-body dualism, I sum up the terms 'soul' and 'mind' here as general reference points. I won't go into the various meanings of the two terms, where the category 'soul' is often reduced to the 'mind' and the same 'mind' sometimes unjustly summarised as a purely psychological category (Van Tuinen, 2023).

3 See: www.nrc.nl/nieuws/2022/09/01/met-microfoons-racisme-in-het-voetbal-bestrijden-a4140501 (visited: 22 August 2023).

4 Neurorights touch on similar issues, see: Ligthart et al. (2021).

Chapter 3

1 Other comparable terms used in this context are 'cybernetic policing' (Tiqqun, (2020 [2001]), 'algorithmic policing' (Wessels, 2023) and 'digital policing' (Fussey & Sandhu, 2022). In the latter case it should be noted that digitalisation and algorithmisation are two separate processes that do not have to coincide.

2 It should be noted here that this procedure can lead to the processing of new facts (intelligence function) to serve future investigations and interventions such as disrupting criminal infrastructures. These secondary objectives have a different goal from traditional evidence collection for the sake of prosecution and trial, raising the question of how these completely different goals should be legally standardised (Schermer, 2022; Hirsch Ballin & Oerlemans, 2023). I return to this in chapter 4.

3 See: https://egmontgroup.org/wp-content/uploads/2022/01/Digital-Transformation-executive-summary.pdf (visited: 1 September 2023).

4 See: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605 (visited: 1 September 2023).

5 See: www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-information-system (visited: 1 September 2023).

6 See: https://blog.ring.com/about-ring/ring-now-part-amazon-family (visited: 30 September 2023).

7 After investigation by the Dutch Data Protection Agency, Tesla made the settings of the security cameras more privacy-friendly. See: https://autoriteitpersoonsgegevens.nl/en/current/tesla-makes-camera-settings-more-privacy-friendly-following-dpa-investigation (visited: 1 September 2023).

8 'The Techno-Feudal Method to Musk's Twitter Madness', https://www.yanisvaroufakis.eu/2022/12/06/the-techno-feudal-method-to-musks-twitter-madness-project-syndicate-op-ed/ (visited: 8 August 2023).

9 There is currently a heated intellectual debate on the pros and cons of the term 'techno-feudalism', see: Morozov (2022).

10 The Amazon Halo (fitness watch with health metrics) and the Amazon Astro Robot (robot on wheels that carries out tasks around the house) can also be connected to the home platform Alexa.
11 See the critical United Nations report 'Racial and xenophobic discrimination and the use of digital technologies in border and immigration enforcement' (2021).

Chapter 4

1 For a good overview of key jurisprudence from the jurisdiction of the European Court of Human Rights with respect to surveillance for criminal prosecution purposes, see: Fedorova et al. (2022).
2 See: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206 (visited: 22 September 2023).
3 Regarding the current use of predictive policing by the Dutch national police, the legislature currently sees no need to regulate its use more closely in the Code of Criminal Procedure (Explanatory Memorandum on the Code of Criminal Procedure, Memorie van toelichting Wetboek van Strafvordering, 2020: 63).
4 Criminologists Tom Snaphaan and Wim Hardyns (2021) have provided insight into the way measuring processes in datasets can give rise to a number of errors, i.e., specification errors, measuring errors and processing errors.
5 Another possibility is the presentation of a chain of evidence when making decisions in the investigation and prosecution of crimes. Such a chain of evidence must then make it clear what

data has been used and what has happened to that data, while all actions carried out with the data should be recorded.

6 The Dutch government also published a toolbox for ethically responsible handling of new technologies: www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nieuwe-technologieen-data-en-ethiek/publieke-waarden/toolbox-voor-ethisch-verantwoorde-innovatie/ (visited: 21 August 2023).

7 Other significant ethical risks include 'ethics shopping', 'ethics lobbying' and 'ethics dumping' (Floridi, 2019).

8 The literature distinguishes three scales of human control, where the human is *in the loop*, *on the loop* or *out of the loop*.

9 The Swedish word 'trygghet' and the German word 'Geborgenheit', which are typically translated into English as 'security,' share similar semantic elements.

Interlude IV

1 In forensic care, the Apple Watch is used to prevent aggression in young people with a short fuse ('biocueing'). The smartwatch monitors a young person's heart rate and vibrates if the tension in the body slowly rises, potentially indicating an oncoming fit of rage. In this respect it strongly resembles what I previously referred to as psychopower.

2 In this context, countless forms of resistance can be distinguished, from political resistance in the form of demonstrations or petitions ('Reclaim Your Face') to everyday resistance such as circumventing digital surveillance (Gilliom & Monahan, 2012; Steijns, 2021).

3 The lack of human contact between police and citizens also became an issue in the German state of Baden-Württemberg, where research has shown that the closure of police stations led to a rise in the number of burglaries and car thefts (Blesse & Diegman, 2022). A similar thing is happening in the case of smart doorbells and cameras to prevent burglaries, which harbour the danger of neighbourhood residents paying less attention to one another and therefore reduced social cohesion, whereas in neighbourhoods with substantial social cohesion and strong mutual control, the chance of burglary is smaller (chapter 3).

4 I borrow the phrase 'coding elite' from Jenna Burrell and Marion Fourcade (2021), who define it as those 'who hold and control the data and software and dwell in the profitable world of money'. I use the term to refer to a group of programmers, coders, data scientists, cloud and software developers, network designers, test specialists and backend developers. For this group, working with AI and algorithms requires different skills and knowledge than were needed in the past to analyse types of crime and perpetrators, for example. They rely less on psychological and social scientific knowledge and are much more data-driven (Schuilenburg & Soudijn, 2023).

5 In his book *Uncomputable*, Alexander Galloway (2021) criticises digital reasoning. With reference to the book's title, he notes in the introduction, 'The excluded term might be "intuition," or it might be "aesthetic experience." It might be the "flesh" or "affect." The excluded term might evoke a certain poetry, mysticism, or romanticism. Or it might simply be life, mundane and unexceptional. "Uncomputable" means all of these things, and more.'

6 For further reference, see: *Wees positief* ('Be positive') by philosopher Richard de Brabander (2022).

Chapter 5

1 In line with this, the literature points to the tension between protection of people in groups and the concept of privacy focused on the individual. Due to the digitalisation and algorithmisation of society, the distinction between individual and mass surveillance is fading and making way for group characteristics and group profiles. Concepts such as group privacy, in which privacy is seen as a collective right, may offer a solution here (Taylor, Floridi & Van der Sloot, 2017).

2 In this text, I have primarily focused on the function of the police and less on areas such as the courts, rehabilitation, forensic care and the prison system, but it should be clear that these domains will also inevitably change due to digitalisation and algorithmisation. See, e.g.: Prins & Roest (2018); Raad voor Strafrechtstoepassing en Jeugdbescherming (2021); Den Boer & Harte (2023).

3 Besides theory, Anderson also reduces politics to quantification. The emphasis on making everything calculable, after all, goes beyond the political choice to weigh up issues of political importance on grounds other than mere technical and economic considerations and with it the question of whether or not to tackle particular social problems. Normative questions play an important role here.

4 A good example and a first step in this direction is the article 'The Biography of an Algorithm' (Glaser, Pollock & D'Adderio, 2021), which proposes a biographical framework for working out the performativity of algorithms in socio-technological assemblages.

5 See also: McGuire & Holt (2017); Smith, Bennett Moses & Chan (2017); Powell, Stratton & Cameron (2018).