

# The Risk of Risk

## Data, Surveillance, and Crime

MARC SCHUILENBURG AND RENÉ VAN SWAANINGEN

FOR years, the Chicago police used the Strategic Subject Algorithm to calculate who was most likely to be a perpetrator or victim of a shooting. This tool was developed by the Illinois Institute of Technology and funded by a grant from the Justice Department's Bureau of Justice Assistance. Scores were calculated and placed on a scale from 0 ("extremely low risk") to 500 ("extremely high risk"). The risk characteristics considered in this process included the number of times a person had been a victim of a shooting incident, the age at last arrest, the number of previous arrests for violent offenses, and whether there were ties to criminal groups (O'Neill 2016). The list included about 1,500 people, whom police said were responsible for most gun violence in Chicago. In 2020, after ten years, the program quietly ended. In a statement, the Chicago police explained this decision:

The general areas of concern in the PTV [Party to Violence] risk model program include: the unreliability of risk scores and tiers; improperly trained sworn personnel; a lack of controls for internal and external access; interventions influenced by PTV risk models which may have attached negative consequences to arrests that did not result in convictions; and a lack of a long-term plan to sustain the PTV models. (*Chicago Sun-Times* 2020)

The Strategic Subject Algorithm is one of many risk assessment tools used by police organizations worldwide to try and predict whether someone will commit a crime. This practice, which may seem like a ludicrous science fiction creation—Minority Report meets Franz Kafka—is known as “predictive policing.” It involves the police attempting to calculate the probability of crime or rule-breaking in a specific area over a certain period and then adjusting police surveillance deployments accordingly (Brayne 2021; Ferguson 2017; Hardyns and Rummens 2018). Besides those systems used in the United States, such as PredPol and HunchLab, the police deploy similar applications in Germany (KrimPro and Precobs), Italy (KeyCrime), and France (Maprevelation). In the Netherlands, the National Police have been working with the Crime Anticipation System (CAS) since 2017, which predicts where and when certain forms of crime may start to occur at the area level. Although these systems do not function the same in each country, they share the characteristic of being about predicting (1) crime risks by using (2) big data and (3) algorithms.

While the introduction of big data and algorithms into policing dates to the 2010s, the phenomenon of predicting “crime risks” goes back much further. During the seventeenth and eighteenth centuries, a new discourse revolved around probability and what we would later call “risk assessment.” This discourse laid the seeds for a type of insurance thinking that slowly but surely permeated law enforcement practice in the twentieth century. This development is generally referred to as “actuarial justice,” which emerged in the last two decades of

the twentieth century, using techniques from the insurance industry to try and predict the risk of criminal behavior (Ericson and Haggerty 1997; Feeley and Simon 1994; Simon 1987, 1988). It involves identifying and classifying individuals based on different degrees of risk to try and prevent acts or behaviors that may threaten a safe and secure society.

This chapter explores relationships between the concepts of risk and crime. Hereto, we first go back to the seventeenth century, as this is where the broader phenomenon of what we today call “risk management” begins, and then we move on to the birth of criminology in the late nineteenth century and early attempts to apply criminological knowledge to the field of law enforcement. Next, we discuss Ulrich Beck’s thesis on the risk society and focus on the phenomenon of actuarial justice. This is followed by a look at the contemporary use of big data and algorithms in policing and their effects on preventing and detecting crime risks. Our conclusion addresses several directions for future thought, research, and action in relation to algorithmic surveillance technologies.

## From Danger to Risk

When we try to draw a historical line leading to the contemporary use of big data in policing, we can distinguish six different frameworks. This development began with a religious frame in which good and evil are distinguished. This distinction goes back to the biblical idea of the Day of Judgement: where those who have lived well will enter heaven if they accept the grace of God, while those who have sinned against God’s commandments will go to hell.

We can also distinguish a biological framework. Assessing danger is a prerequisite for human survival. When we fail, we fall prey to all kinds of dangers, from wild animals that attack us to getting too close to a fire that burns us. From learning to avoid danger, we arrive at a philosophical framework inspired by the Enlightenment, in which we start to *measure* risks. Where people initially understood risks as dangers beyond human control and attributable to fate or divine providence, we now speak about risks in terms of decisions that people and organizations consciously make and that can have unintended consequences. These consequences derive from developments that we ourselves have set in motion. A critical difference between “danger” and “risk” is that we no longer accept that we must resign ourselves to fate (Castel 1991). The word “risk” comes from the Italian *risicare*, which means, among other things, “to dare,” and in this sense, it indicates having a choice (Bernstein 1998, 8).

The rise of statistics in the sciences was the next phase in this development, in which we also see techniques emerging to estimate risks. At that time, the rise of what we call “probabilistic logic” also occurred. The genealogy of this conceptualization of risk takes us back deep into the seventeenth century. In his book *Against the Gods*, Peter Bernstein (1998) observes that all the tools we use today in risk management and analyzing important decisions and choices stem from 1654 to 1760. Evidence of this can be found in the correspondence between French mathematician and physicist Blaise Pascal and the legal scholar Pierre de Fermat in 1654. In their letters, they outline probability theory for the first time, with Pascal concluding that probabilities cannot be compared with arithmetic proportionality principles. Partly because of Pascal’s findings, probability theory became an important scientific field within a few years. In 1660, for instance, the Dutch mathematician and physicist Christiaan Huygens published a text on probability in Frans van Schooten’s book *Mathematische Oeffeningen* (Mathematic Exercises) entitled *Van Rekeningh in Spelen van Geluck* (On Calculation in Games of Luck).

This probabilistic logic requires collecting, processing, and interpreting data systematically. These developments constitute the next step toward modern risk assessment, as

prediction is increasingly based on data. In the process, actuarial thinking comes to the forefront. The seeds for this were sown as early as the seventeenth century. Grand Pensionary Johan de Witt, the highest official of the States of Holland, applied Huygens's ideas in his work for an insurance company. In his treatise on annuities, entitled *Waerdye van Lijfrenten naar Proportie van Losrenten* (Value of Annuities in Proportion of Redemption Interests), which he presented to the states of Holland and Friesland in 1671, De Witt outlined a theory of a variable annuity. Such annuities involve a person receiving an annual payment from a sum of money made available to the government. Detailed statistics on mortality rates allowed the government to calculate how much they had to pay as an annuity from a given deposit.

Insurance policies linked the mathematical foundations of the concept of risk with the probability of payment. In fact, "risk" is a neologism of what was initially called "insurance" (Ewald 1990). In other words, nothing is a risk in itself. Risk only exists in relation to a calculated chance. Whereas in everyday parlance, risk is synonymous with danger, in insurance thinking, risk is associated with notions of chance, probability, eventuality, and liability. Risk then indicates a specific approach toward certain events that may happen to a group or to several individuals. Therefore, François Ewald (1990, 2002) distinguishes three characteristics of the concept of risk. Risk is calculable, collective, and it represents capital.

Advances in computing technology and artificial intelligence (AI) heralded the final step toward today's algorithmic surveillance. This commenced with the increased public availability of computers at the end of the twentieth century and started to dominate in the twenty-first century as computing power increased dramatically and AI and assorted machine learning algorithms, with the capacity to learn independently and make decisions, emerged (Murphy 2017; Kosta 2022; Schuilenburg 2024).

Distinguishing these seven developments in our walk through the history of risk-thinking, we can see that the distinction between "good" and "evil" and the assessment of danger has always existed and that developments in statistics, insurance, computers, and AI contribute to our ability to calculate risks. In the next section, we demonstrate how the selection of groups that are at a statistically higher risk of committing crime or reoffending has been occurring since the beginning of criminology in the second half of the nineteenth century and how, by the end of the twentieth century, the use of actuarial methods in crime control led to a focus on the so-called three p's of prevention, precaution, and preemption.

## From Preemptive Crime Control to Actuarial Justice

Identifying dangerous individuals and groups and taking preemptive measures against them dates to the early days of criminology. In a historical study on surveillance, Pieter Leloup (2023, 36) argues that in current discussions about "dataveillance," many old questions are emerging in a new guise. Leloup states:

After all, surveillance encompasses similar types of activities, both in the pre-digital and in the digital form. This includes collecting and storing information, supervising individuals and controlling the behavior of those who are under surveillance.

A revolution in surveillance did, however, occur in the second half of the nineteenth century. In 1879, Césaire Lombroso's typologies of perpetrators, Adolphe Quetelet's concept of the "average person," and the development of photography inspired the forensic expert of the Parisian police, Alphonse Bertillon, to develop a system for identifying persons. This system

was named *Bertillonage* after him and was used worldwide. Leloup (2023, 37) notes how the new technology of photography meshed with emergent policing ambitions:

New developments in crime and crime control stimulated (. . .) a wider application of photography. The combination of rising crime rates and the increased mobility of offenders and offender groups required the introduction of an efficient and faster exchange of information between police forces.

Beginning in the 1870s, these developments contributed to the establishment of a so-called scientific police in many European countries.

Austrian criminal law scholar Hans Grosz took the next step in professionalizing criminal investigation. In 1893, Grosz held the first chair in criminalistics and was one of the first to systematize questions about the “who, what, where, with what, why, how, when” of crime, as he aimed to professionalize the criminal investigation department. Grosz established the *Archiv für Kriminologie, Kriminalantropologie und Kriminalistik* (Archives of Criminology, Criminal Anthropology, and Criminalistics) in 1898 to serve this purpose (Wetzell 2000, 61).

In line with these developments, Germany established the *Internationale Kriminalpolizeiliche Kommission* (IKK, International Police Committee) in 1923 to investigate the risk profiles of criminals operating internationally, people trafficking in women and narcotics, pornography distributors, car thieves, and groups of people, such as Jews and “gypsies” (Roma, Sinti). The IKK was meant to prioritize the investigation of these crimes and populations, and it is the predecessor of today’s Interpol. The IKK sought to design preventative measures to protect society against specific groups who were thought to have a high risk of engaging in the aforementioned international crimes. Jews and “gypsies,” for example, were seen as major risk groups, because they form an international diaspora, rather than a “people” (“Volk” in German) that “belongs” to a specific country.

In 1941, in the middle of the Nazi era, and at the instigation of Heinrich Himmler, Robert Ritter established a unique research institute, the *Kriminalbiologisches Institut* (Institute for Criminal Biology), to provide the so-called security police (*Sicherheitspolizei*) with scientific knowledge about risk groups (Wetzell 2000, 220). In his book *Criminology and the Criminal Justice System*, Cyrille Fijnaut (2017, 332) comments on this development:

Criminal biology was no longer intended to make individualization of punishment and treatment of offenders possible, but rather above all served to identify those members of the population who—because of their genetic and racial characteristics—constituted a supposed serious danger to the community and who therefore needed to be systematically eliminated.

In his history of German criminology between 1880 and 1945, Richard Wetzell (2000) argues that in this way “the criminal” is “invented.”

The concentric zone models produced by Clifford Shaw and Henry McKay in their foundational contributions to the late nineteenth-century Chicago School of Sociology prefigure the rise of geographical profiling and mapping hot spots. Bruce Arrigo et al. (2020, 503) locate “the earliest forms of preemptive policing” in “the examination of geographical crime patterns (which) led to the police practice of crime mapping with push-pin wall maps.” Bernard Harcourt (2007, 39) also situates the beginnings of modern actuarial methods in criminal justice and prediction studies in criminology, which Ernest Burgess initiated in 1928 with a project on parole.

Several sociological developments explain why, despite all these precursors of risk assessment in criminal justice, it took until the end of the twentieth century before we started

talking about “actuarial justice.” These developments begin with Max Weber’s insights into the disenchantment of the modern world and the rationalization of governance. This is also the starting point for Ulrich Beck’s thesis on the emergence of the risk society. When fixed administrative structures gave way to more flexible networks, the Weberian rationalization process underwent a kind of radicalization. Beck defines “risk” as “a systematic way of dealing with hazards and insecurities induced and introduced by modernization itself” (1992, 21). He argues that the social production of risk coincided with the social production of health and wealth.

Other key contributing factors are tied to processes associated with what Zygmunt Bauman calls “liquid modernity.” He posits that we have moved away from a “solid” modern utopia to a “light” modernity in which freedom leads to greater levels of anxiety and insecurity. In his book *Liquid Fear*, Bauman (2006) focuses on how—where we fail to tame the uncontrolled forces of the social and natural worlds—an unpredictable uncertainty remains. This uncertainty is almost unbearable for late-modern (wo)man as (s)he prefers to measure and record *everything*. As the technical possibilities for such documenting and recording have increased, we have become more and more obsessed with measuring, rating, and ranking almost all areas of our lives, from watches that constantly measure our heart rate (Apple Watch and Fitbit) to endlessly checking our “status update” and our “likes” on social media, to pushing a red, yellow, or green smiley to indicate the cleanliness of a public toilet. A striking range of things are mapped out with the implicit assumption that doing so provides more control, which can then be used to improve things.

It is also worth noting the enormous progress in mapping, systematizing, and processing technologies compared with the 1870s, when the first “scientific police departments” were established in Europe. Leloup (2023, 42) notes in this respect:

The technological, computational and organisational capacities were only in few respects comparable to those of today. The intensity and scope of surveillance also increased sharply over time. Especially under the influence of the latest technologies and practices of digital surveillance, such as dataveillance, this practice has penetrated even more deeply into our society and into our lives.

Bruce Arrigo et al. (2020, 508) call this the “ultramodern era of digital inter-connectivity” because it extrapolates modern ideas about the calculability of risk to use algorithms as both the source and product of dataveillance and algorithmic surveillance.

According to Jude McCullough and Sharon Pickering (2009), this algorithmic revolution in applying actuarial techniques in policing truly gained momentum when methods from antiterrorism policy and national intelligence organizations were introduced into regular policing. They argue that this development has also led to a new form of criminalization through the overpolicing of low-income communities of color. Charlotte Heath-Kelly (2017) shows how such scrutiny mainly focuses on areas where many Muslims live, producing a criminalization of Muslim neighborhoods. It is also worth noting that many nations introduced biometric passports shortly after the terrorist waves of the early 2000s, which were soon used primarily to combat irregular migration.

Years after antigovernment extremist and white supremacist Timothy McVeigh’s attack in Oklahoma in 1995, years after neo-Nazi Anders Breivik’s attacks in Oslo and Utøya in 2011, and even years after the Christchurch Mosque shootings in 2019, the extreme right finally came into the sights of the security services. Only recently has the threat of antigovernment thinking become a central concern of security agencies. Such threats gained enhanced momentum during the COVID-19 pandemic, when people from traditionally high trust

societies came to see the state as an institution that was limiting their freedom and trying to control their daily lives. In the Netherlands, for example, which is traditionally a high trust society, there was evidence of a decreased trust in government after the threat of the virus had declined (Engbersen et al. 2021).

## Actuarial Justice and Its Risks

Malcolm Feeley and Jonathan Simon coined the term “actuarial justice” in 1994, although they did not define it. Instead, they argued:

Actuarial justice is nebulous, but it is significant. Actuarial justice involves how we conceive of and talk about crime policy, but it is not an ideology in the narrow sense of a set of beliefs and ideas which constrain action. It involves practices but is not reducible to a specific technology or set of behaviors. Indeed, it is powerful and significant precisely because it lacks a well-articulated ideology and identification with a specific technology. (1994, 174)

That the use of actuarial, probabilistic, statistical models in the criminal justice system is by no means new was demonstrated in the previous section(s). Feeley and Simon (1994, 174) also do not claim to have discovered something “new,” but argue that they were pointing to “partial practices which have had long and varied histories. Their newness lies in their particular combinations and the particular micro-practices they are embedded in and the functions which they perform.” The broad, if not systematic, practical application of risk assessment models probably started in medical science and was then adopted in psychology and eventually in criminology, especially in penology.

Bruce Arrigo et al. (2020, 504) argue that within the criminal legal system, “actuarial techniques are devised to identify, classify, and control people grouped by varying degrees of dangerousness.” An early Dutch example of such processes is the RISC (Risk Assessment Scales—*Risico Inschatting Schalen*), introduced by the Probation Service in 2004. This system distinguishes twelve domains where risks of recidivism can arise. It is a risk assessment model that relies on inputs of correlations highly associated with criminal offending. The level of risk this process assigns to a person ultimately determines what measures officials will employ to manage an individual’s future risk of committing a crime: behavioral intervention, custodial sentence, clinical treatment, and so on. The introduction of this system has gone hand in hand with the popularization of the “what works” and “best practices” approach within criminal justice, which is also derived from medicine and psychology. Within such a framework, funding decisions are based on determining what practices *work* according to a set of specific criteria.

In his 2007 study *Against Prediction*, Bernard Harcourt pointed out four dangers of applying actuarial prediction techniques in policing and crime politics: (1) an overdose of information could lead to *less* effective law enforcement because officers must check all kinds of empty leads; (2) a self-fulfilling prophecy is possible when a person’s criminal history is used as a proxy in prediction models; (3) normative assumptions and ingrained stereotypes become invisible through reliance on a technical logic; and (4) the use of risk profiles prepares for selective incapacitation, as it relies on *categories* of people defined as societal risks, it encourages penal policies focused on removing particular groups from society.

With the rise of exponentially increased computer power and AI, the twenty-first century is witnessing a movement from focusing on statistical correlations to using self-learning algorithms. Pioneering in this regard is the 1997 study *Policing a Risk Society* by Richard Ericson and Kevin Haggerty. They argue that policing has mainly become a form of risk

communication. In our highly fragmented societies, police work has shifted from traditional crime control and order maintenance modes toward providing security through surveillance technologies designed to identify, predict, and manage risks. In line with Ulrich Beck's theory of the risk society, Ericson and Haggerty (1997, 6) state:

Risk society operates within a negative logic that focuses on fear and the social distribution of “bads” more than on progress and the social distribution of “goods.” Collective fear and foreboding underpin the value system of an unsafe society, perpetuate insecurity, and feed incessant demands for more knowledge of risk.

They also explicitly place the development of “system surveillance” in the framework of actuarial justice (Ericson and Haggerty 1997, 52).

As actuarial justice started to gain a solid foothold in Western society, scholars explicitly placed it in the context of Beck's notion of a risk society. In the Netherlands, for example, actuarial justice has always been characterized as “risk justice”—something also attributable to the fact that the term “actuarial” is not actually used in Dutch outside the insurance world (van Swaaningen 1996). In the Dutch situation it is interesting that, in addition to the penological domain, risk thinking has already been applied in drug policy, not only with regard to profiling user populations but also in reducing the harms that come with criminalizing drugs.

As far as the dangers of thinking in terms of “risks” are concerned, scholars have pointed to the fallacious assumption that “crime” can be treated as a value-neutral problem, given that all kinds of normative assumptions and partisan political charges surround criminal activities. It is somewhat strange to assume that the fear of crime—which often has irrational aspects—could be dealt with rationally. Negative public opinions about certain groups of citizens (drug addicts but also social benefits recipients or migrants) continue to cast their shadow on “the system,” resulting in such individuals often being treated as potential fraudsters (van Swaaningen 1996, 84–85). There is also the prospect that the actuarial promise of enhanced safety carries with it a certain insatiability—the safer things become, the more pressure there is to eliminate even the slightest “dangers” and “risks.” In his book *Hysteria*, Marc Schuilenburg (2021, 138) called this the “success paradox”—“The wealthier, healthier and safer our lives become, the more hysterical the last residue of lack makes us feel.”

In her article “Pre-Crime and Post-Criminology?” Lucia Zedner (2007) points to other reasons why it is politically necessary to critically interrogate the public demand for security. One consequence of this trend is that crime control has become increasingly opaque as more and more non-state actors have become involved in providing security. In part, this has been encouraged by the “New Public Management” ideology and the related trend toward “responsibilization” (Garland 2001; Schuilenburg 2015).

A significant problem with risk thinking in crime control is that officials overestimate the possibilities of predicting crime. In fact, Zedner argues that such “predictability” does not really exist. Despite the significantly increased technical possibilities to map risks and correlations with delinquent behavior, academic faith in the ability to predict such behavior has decreased rather than increased. However, such aspirations remain immensely popular in police and judicial practice, as is apparent, for example, in the case of the current use of predictive policing.

Our historical retrospective has shown the origins of mapping and managing security risks. The question that now emerges is how far we are from moving beyond the scientific police of the second half of the nineteenth century to the vision of a pre-crime police department of 2054.

## Big-Data Policing: Three Typologies

Big data, algorithms, and AI have revolutionized many domains in late- or ultra-modern society. Law enforcement is no exception. Several authors have pointed to a current transition in policing from reliance on actuarialism to using big data analytics to detect crime risks (e.g., Ferguson 2017; Moses and Chan 2018; Chan and Moses 2017). In *Surveillance After Snowden*, David Lyon writes, “Surveillance today cannot be understood without a sense of how the quest for ‘big data’ approaches are becoming increasingly central” (2015, 68–69). By using big data, algorithms, and AI, the police aspire to become better at acting proactively, reduce their reliance on human judgment, and significantly improving their efficiency in preventing and detecting crime.

Such developments have given rise to talk of “big-data policing,” which refers to trying to make society safer by accessing and analyzing large volumes of data through assorted algorithms (Schuilenburg and Soudijn 2023). Big data has several features, including a large “volume” of data, an increased “velocity” at which data are collected, the use of “unstructured” and “varied” data, and the fact that those data are “digital” (Laney 2001; Gartner 2011; Ridgeway 2018). Given the sheer scale of information involved, algorithms are needed to collect and process the data and to produce a conclusion or offer advice (Pasquale 2015; Danaheer et al. 2017).

Let us first discuss some of the difficulties in using the term “algorithm,” a term that dates back to the ninth century and the Persian mathematician Al-Khwarizmi (Peeters and Schuilenburg 2021). Basically, an algorithm is a set of instructions that leads to calculating an outcome for a problem. It can be compared to a recipe: By following a series of fixed steps, you prepare a dish you can place on the table. In practice, there are different types of algorithms. The simplest are called “rule-based,” which use formulas of the kind “if A, then B.” More complex “self-learning” algorithms aim to achieve a specific goal without explicit instructions. These include “machine learning” and “deep learning,” which can be divided into different forms (“supervised,” “semi-supervised,” or “unsupervised”) (Atilla and Sathiyamoorthi 2020). One danger of self-learning algorithms is that they can lead to a loss of human control. Franks Pasquale (2015) speaks of a “black box scenario,” where decision-making processes are not only inaccessible to outsiders and thus uncontrollable but are no longer understood or explainable by users. Such opacity is a vital social and political concern about using such techniques.

Police organizations use three types of big-data tools (Schuilenburg and Soudijn 2023). First are those used to examine the past. “Retrospective tools” are used, among others, in crime detection, especially when large amounts of data need to be analyzed. A well-known example involved the authorities reading millions of intercepted crypto messages on the encrypted messaging platform EncroChat, often used by criminal organizations. A joint investigation—initiated by French and Dutch authorities—intercepted and analyzed over 115 million conversations using big-data tools trained to filter the data by priority and which can find connections relevant to criminal investigations (Europol and Eurojust Public Information 2021). Such retrospective tools have provided data for hundreds of ongoing investigations into crimes committed in the past and to opening completely new criminal investigations. The police characterize such developments as a “game changer” (Stoker 2020).

Second, the police use “real-time” (“here-and-now”) big-data tools. These include facial recognition cameras in public spaces, which identify individuals by comparing someone’s face against a computer database of known faces. The targets of such scrutiny range from convicted criminals to asylum seekers. In the street, police officers in some jurisdictions

wear body cameras, which include real-time facial recognition technology that “will allow police to know about active warrants, prior violence, or generally peaceful conduct (just like the fixed camera)” (Ferguson 2017, 89). Police officers also have access to various linked police apps on their smartphones that tell them whether an identified person has an outstanding fine and what is happening on social media in the neighborhood. Another example of a real-time big-data tool is the so-called web crawlers (also known as spiders or spider-bots), used by the police to search the dark web for, among other things, child pornography or drug trafficking.

Third, police organizations are using big-data tools to “predict” where, when, and by whom crimes are more likely to be committed (Perry et al. 2013; Van Brakel 2016; Bennett Moses and Chan 2018). These applications are “future-looking tools” and are used for predictive, rather than reactive or explanatory, purposes (Brayne 2017). By using these tools, 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. Remarkably, there are hardly any robust empirical studies of the effects of these predictive applications. In several American cities, the application of predictive policing has been found to be effective, while in other countries, including the Netherlands, no demonstrable effect has been shown on crime levels (Mohler et al. 2015; Mali et al. 2017; Meijer and Wessels 2019; Ratcliffe et al. 2021).

As different as the three types of big-data tools are, they are all embedded in a discourse in which the presumed technical and economic advantages of algorithms and AI prevail. This orientation focuses on issues such as the speed with which data can be collected or on efficiency arguments, with work processes and risk management being seen as comprehensively improved by using big-data applications. Although it makes sense that effectiveness and efficiency are highly valued in risk management, the reality generally differs from the expectations. Limitations in the efficiency of such initiatives exist because these tools must always be considered in the context of the social and cultural environment in which they are embedded (Schuilenburg 2024). Such contexts give rise to at least three areas of social concern, which are the focus of the next section.

## Risks of Big-Data Policing

From the burgeoning literature on the police use of big-data tools to prevent and detect crime risks, we discern three domains of social concern: (1) a focus on efficiency, (2) the eradication of social knowledge, and (3) the production of ethical, legal, and societal risks.

The focus on efficiency is not exclusive to big-data policing. Sociologically, it can be traced back to a particular form of rationality based on notions of calculability and predictability addressed above. In such an orientation, costs and benefits are ideally balanced, and scarce resources are used more efficiently to optimize outcomes. Max Weber ([1921/1922] 2006) long ago contrasted goal-based rational action (*zweckrational*) with value-based action (*wertrational*). Weber pointed to how instrumental goal rationality had become increasingly dominant with the rise of modernity and contributed to the bureaucratization of the state apparatus. He spoke of an “iron cage” (*stahlhartes Gehäuse*) in which instrumental rationality left little room for personal and emotional considerations in decision-making.

In an update of Weber’s analysis, there is now talk of a “digital cage”: an information architecture that hinges on big data and algorithms instead of bureaucratic rules and procedures (Peeters and Widlak 2018). Such technocratic governance is embedded in “solutionism” (Morozov 2013) and “AI common sense” (Aradou 2023)—a strong belief that technology

provides *the* solution to societal problems such as ensuring safety. Claudia Aradou critically points out that for such advocates, “the question of whether AI is appropriate at all, becomes unthinkable, as asking it would interrupt the move towards more digital technology, more data, more interoperability and more AI” (2023, 303). Such views tend to be based on the questionable assumption that technology is value-neutral.

Regardless of the empirical consequences of these changes, in a “digital cage”—or rather, an “algorithmic cage” (Schuilenburg 2024, 54)—the legitimacy of police action shifts from being based on traditional rules and procedures to invisible algorithms. Frank Pasquale argues that in this context, “authority is increasingly expressed algorithmically” (2015, 8). This all raises questions about what institutional mechanisms need to be developed to guarantee that big data, algorithms, and AI will not erode police legitimacy, which depends on citizens trusting in the fairness of police actions.

The second social concern relates to the eradication of social knowledge in data-driven police work. Marc Schuilenburg and Melvin Soudijn (2023) note that working with big data, algorithms, and AI requires the police to have different expertise and skills than those used to create and operate the risk and actuarial systems they have traditionally relied upon to analyze and predict crime trends. In contrast to actuarial tools, the design and use of big-data tools means that police organizations rely less on psychological and social scientific knowledge than was historically the case. Kelly Hannah-Moffat (2019, 458) compares these different approaches, pointing out that, among other things:

The technologies differ in the size of the population from which their results are based: psychology informed risk tools are based on statistical analyses of a sample of a population, whereas big data informed risk algorithms are based on massive and potentially infinite population data.

It is also the case that psychological and social scientifically informed risk tools are built on preconceived theoretical or disciplinary norms and established scientific methodologies. Conversely, big-data tools rely on information gathered from diverse sources and compiled and examined “with little attention to social scientific methodological standards, and with limited substantive knowledge of the subject matter” (2019, 458; see also Castro-Toledo et al. 2023).

Data-driven police work also requires new skills in certain police functions, including mastery of programming languages and technical skills to design new big-data tools (Haggerty 2004). Such specialist and technical knowledge make overly tight control and management methods difficult and will, in practice, lead to a sizeable discretionary space for certain police functions, as is the case with programmers, coders, cloud and software developers, network designers, and test specialists. The literature mentions 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” (Schuilenburg 2024, 120–121). The emergence of this coding elite makes the question of how police leadership can manage such work relevant. Examples include biometric facial recognition tools, which automatically compare facial features to identify unknown suspects from photographs and closed-circuit television. Critics have identified many problems with these tools: racial bias, privacy violations, identity theft, and secrecy, to name a few (e.g., Bowyer 2004; Fussey and Murray 2019; Smith and Miller 2022). It is unclear whether police officials are well-positioned to address such concerns.

This brings us to a third social issue: the production of ethical, legal, and societal risks. Despite the growing use of big-data tools in safety and security management, there is also

much uncertainty about the risks they might be producing. Heightened risks include loss of privacy, discrimination against minorities, and identification of at-risk groups based on inappropriate or irrelevant characteristics and categories (e.g., Ferguson 2017; Peeters and Schuilenburg 2018; Benjamin 2019). In *Race After Technology*, Ruha Benjamin speaks of “the New Jim Code” and how such technologies can allow “racist habits and logics to enter through the backdoor of tech design” (2019, 160). Critics also regularly raise concerns about the rule of law in big-data policing. Such issues range from the problem of dirty data and fishing expeditions to the violation of the principle that people should be presumed innocent (e.g., Kraft 2018; Richardson, Schultz, and Crawford 2019; Schuilenburg 2021). Other studies have shown that applying big-data tools can lead to “machine justice” (Peeters and Schuilenburg 2018)—the paradox that self-learning algorithms create an impression of a decision-making process constantly in motion, while in fact potentially leading to strict and disciplined compliance with the results.

Consequently, regulators have increasingly targeted these tools, passing international legislation to enhance public values such as nondiscrimination and algorithmic accountability. As noted by the High-Level Expert Group on Artificial Intelligence of the European Commission in *Ethics Guidelines for Trustworthy AI* (2019), public principles such as “respect for human autonomy,” “prevention of harm,” “fairness,” and “explicability” are becoming increasingly important for police organizations when developing new big-data tools.

## Conclusion: Exploring Research Challenges

In this chapter, we have discussed the genealogy of the concept of risk in the field of safety and security management. We have traced the discourse on risk tools to the seventeenth century and pointed out the differences between notions of “danger” and “risk.” Dangers were historically considered beyond human control and attributed to fate or divine providence (“will of God”). Now, we speak of risks in terms of actions and decisions that people make, which may have unintended consequences. The discourse on risk influenced police practice from the late nineteenth century onward, but it only became a key development in the criminal legal system in the 1980s. To explain the increased use of actuarial techniques, police officials, politicians, and administrative criminologists alike have pointed to a sharp rise in recorded crime, both in quantity and severity, and a changing cultural and political climate. These developments have contributed to a risk-obsessed society in which safety is defined as the absence of risk. As a result, criminal law is evolving into a more proactive instrument, with preemption becoming more central to judicial action.

From the police to the prison to probation services, criminal justice institutions use all kinds of risk assessment tools to try and prevent crime and reduce the likelihood of victimization and recidivism. Initially, the validity of actuarial tools in supporting criminal decision-making was based on social scientific knowledge, most notably from psychology. However, risk assessment tools based on big data rely less directly on psychological and social scientific knowledge. Instead, they collect information from a multitude of data sources by using increasingly sophisticated techniques that can unlock and connect even the smallest data sets. Consequently, a coding elite appears to have emerged, responsible for designing and developing new tools based on big data and shaping decisions about which datasets to analyze and the algorithms to use to process those data.

To conclude, the relationship between risk and crime in the contemporary era cannot be understood without a sense of how law enforcement agencies increasingly use big data, algorithms, and AI in their decision-making processes. An important question that emerges,

but which is not fully explored in the literature, is what big-data tools exist and which organizations are using them? Big-data tools are not only used by national police organizations but also by organizations “above” (Europol and Interpol, for example), “beyond” (probation services, prison system, and private companies), and “below” the police. In the latter case, one can think of citizens patrolling a neighborhood guided and informed by specially designed apps (Schuilenburg and Soudijn 2023; Schuilenburg 2024). More scientific research is needed on how all these parties use big-data tools and their consequences for safety and security management.

More research is also needed into the ethical, legal, and societal considerations relating to the growing use of new surveillance technologies to detect crime risks, including empirical methods to evaluate how police use such devices. With big-data tools becoming an increasingly regular part of police investigations, we need to examine how these technologies can be managed and controlled within a framework guided by the values of a democratic society. In criminology, there have been few robust empirical studies into the effects of big-data tools. Considerations of the normative frameworks for approaching AI in relation to security are unclear or even completely absent (Schuilenburg 2024). Such a situation is remarkable because, as we have shown, there are pressing ethical, legal, and societal issues related to new risk technologies. Concerns about privacy, the prospect of bias, and the abuse of power are entirely legitimate.

Finally, more social scientific research on the AI experiences of those dealing with big-data tools is needed. AI is as much a social practice as a technical issue. Consequently, the experiences of individuals who come into contact with big-data tools—from police officers and judges to citizens deemed to be a “high risk”—must be involved in scientific research on the subject. Only then will we better understand what big data and algorithms can do and what they do to us.

## References

- Aradou, Claudia. 2023. “Borders Have Always Been Artificial: Migration, Data and AI.” *International Migration* 61: 303–306.
- Arrigo, Bruce, Brian Sellers, and Jo Sostakas. 2020. “Pre-crime, Post-criminology, and the Captivity of Ultramodern Desire.” *International Journal of the Semiotics of Law* 33: 497–514.
- Atila, Elci, and Velayutham Sathiyamoorthi. 2020. *Challenges and Applications of Data Analytics in Social Perspectives*. IGI Global.
- Bauman, Zygmunt. 2006. *Liquid Fear*. Polity Press.
- Beck, Ulrich. (1996) 1992. *Risk Society: Towards a New Modernity*. Sage.
- Benjamin, Ruha. 2019. *Race After Technology: Abolitionist Tools for the New Jim Code*. Polity Press.
- Bernstein, Peter. 1998. *Against the Gods. The Remarkable Story of Risk*. John Wiley & Sons.
- Bowyer, Kevin. 2004. “Face Recognition Technology: Security versus Privacy.” *Technology and Society Magazine* 23(1): 9–19.
- Brayne, Sarah. 2017. “Big Data Surveillance: ‘The Case of Policing’.” *American Sociological Review* 82(5): 977–1008.
- Brayne, Sarah. 2021. *Predict and Surveil. Data, Discretion, and the Future of Policing*. Oxford University Press.
- Castel, Robert. 1991. “From Dangerousness to Risk.” In: *The Foucault effect: Studies in Governmentality*, edited by Graham Burchell, Colin Gordon, and Peter Miller. University of Chicago Press.
- Castro-Toledo, Francisco, Fernando Miró-Llinares, and Jesús Aguerrí. 2023. “Data-driven Criminal Justice in the Age of Algorithms: Epistemic Challenges and Practical Implications.” *Criminal Law Forum* 34: 295–316.

- Chan, Janet, and Lyeria Bennett Moses. 2017. "Making Sense of Big Data for Security." *The British Journal of Criminology* 57(2): 299–319.
- Chicago Sun-Times. 2020. "CPD Decommissions 'Strategic Subject List'." January 27.
- Danaher, John, Michael Hogan, Chris Noone, et al. 2017. "Algorithmic Governance: Developing a Research Agenda Through the Power of Collective Intelligence." *Big Data & Society* 4(2): 1–21.
- Engbersen, Godfried, Marianne van Bochove, Jan de Boom, et al. 2021. *De laagvertrouwensamenleving. De maatschappelijke impact van COVID-19 in Amsterdam, Den Haag, Rotterdam & Nederland, vijfde meting*. Erasmus School of Social and Behavioural Sciences & Kenniswerkplaats Leefbare Wijken.
- Ericson, Richard, and Kevin Haggerty. 1997. *Policing the Risk Society*. University of Toronto Press.
- Europol & Eurojust Public Information. 2021. *Third Report of the Observatory Function on Encryption*. <https://www.europol.europa.eu/publications-events/publications/third-report-of-observatory-function-encryption>
- Ewald, François. 1990. "Norms, Discipline, and the Law." *Representations* 30: 138–161.
- Ewald, François. 2002. "The Return of Descartes's Malicious Demon: An Outline of a Philosophy of Precaution." In *Embracing Risk. The Changing Culture of Insurance and Responsibility*, edited by Tom Baker and Jonathan Simon. University of Chicago Press.
- Feeley, Malcolm, and Jonathan Simon. 1994. "Actuarial Justice: The Emerging New Criminal Law." In *The Futures of Criminology*, edited by D. Nelken. Sage.
- Ferguson, Andrew. 2017. *The Rise of Big Data Policing. Surveillance, Race, and the Future of Law Enforcement*. New York University Press.
- Fijnaut, Cyrille. 2017. *Criminology and the Criminal Justice System: A Historical and Transatlantic Introduction*. Intersentia.
- Fussey, Peter, and Daragh Murray. 2019. *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, University of Essex.
- Garland, David. 2001. *The Culture of Control: Crime and Social Order in Contemporary Society*. University of Chicago Press.
- Gartner. 2011. "Gartner Says Solving 'Big Data' Challenge Involves More Than Just Managing Volumes of Data." [www.businesswire.com/news/home/20110627005655/en/Gartner-Says-Solving-Big-Data-Challenge-Involves-More-Than-Just-Managing-Volumes-of-Data](http://www.businesswire.com/news/home/20110627005655/en/Gartner-Says-Solving-Big-Data-Challenge-Involves-More-Than-Just-Managing-Volumes-of-Data)
- Haggerty, Kevin. 2004. "Displaced Expertise: Three Constraints on the Policy Relevance of Criminological Thought." *Theoretical Criminology* 8(2): 211–231.
- Hannah-Moffat, Kelly. 2019. "Algorithmic Risk Governance: Big Data Analytics, Race and Information Activism in Criminal Justice Debates." *Theoretical Criminology* 23(4): 453–470.
- Harcourt, Bernard. 2007. *Against Prediction. Profiling, Policing, and Punishing in an Actuarial Age*. University of Chicago Press.
- Hardyns, Wim, and Anneleen Rummens. 2018. "Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges." *European Journal on Criminal Policy and Research* 24: 201–218.
- Heath-Kelly, Charlotte. 2017. "The Geography of Pre-Criminal Space: Epidemiological Imaginations of Radicalisation Risk in the UK Prevent Strategy, 2007–2017." *Critical Studies on Terrorism* 10(2): 297–319.
- High-Level Expert Group on Artificial Intelligence. 2019. *Ethics Guidelines for Trustworthy AI*. European Commission.
- Kosta, Eleni. 2022. "Algorithmic State Surveillance: Challenging the Notion of Agency in Human Rights." *Regulation & Governance* 16(1): 212–224.
- Kraft, Oliver. 2018. *Sharpening the Money-Laundering Risk Picture: How Data Analytics Can Support Financial Intelligence, Supervision and Enforcement*. Royal United Services Institute for Defence and Security Studies (RUSI).
- Laney, Doug. 2001. "3D Data Management: Controlling Data Volume, Velocity and Variety." *META Group Research Note* 6.
- Leloup, Pieter. 2023. "De historiseren van [digitale] surveillance. Fotografie als middel van toezicht en controle." *Tijdschrift over Cultuur & Criminaliteit* 13(2): 33–49.

- Lyon, David. 2015. *Surveillance After Snowden*. Polity Press.
- Mali, Bas, Carla Bronkhorst-Giesen, and Mariëlle den Hengst. 2017. *Predictive policing: lessen voor de toekomst. Een evaluatie van de landelijke pilot*. Politieacademie.
- McCulloch, Jude, and Sharon Pickering. 2009. "Pre-Crime and Counter-Terrorism. Imagining Future Crime in the 'War on Terror'." *The British Journal of Criminology* 49(5): 628–645.
- Meijer, Albert, and Martijn Wessels. 2019. "Predictive Policing; Review of Benefits and Drawbacks." *International Journal of Public Administration* 42: 1031–1039.
- Mohler, George, Martin Short, Sean Malinowski, and Mark Johnson. 2015. "Randomized Controlled Field Trials of Predictive Policing." *Journal of the American Statistical Association* 110(512): 399–1411.
- Morozov, Evgeny. 2013. *To Save Everything, Click Here*. Public Affairs Books.
- Moses, Lyria Bennett, and Janet Chan. 2018. "Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability." *Policing and Society* 28(7): 806–822.
- Murphy, Maria. 2017. "Algorithmic Surveillance: The Collection Conundrum." *International Review of Law, Computers & Technology* 31: 225–242.
- O'Neill, Cathy. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Penguin.
- Pasquale, Frank. 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press.
- Peeters, Rik, and Marc Schuilenburg. 2018. "Machine Justice: Governing Security Through the Bureaucracy of Algorithms." *Information Polity* 23(3): 267–280.
- Peeters, Rik, and Marc Schuilenburg. 2021. The Algorithmic Society: An Introduction. In *The Algorithmic Society: Technology, Power, and Knowledge*, edited by Marc Schuilenburg and Rik Peeters. Routledge.
- Peeters, Rik, and Arjen 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, Walter, Brian McInnis, Carter Price, Susan Smith, and John Hollywood. 2013. *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. RAND Corporation.
- Ratcliffe, Jerry, Ralph Taylor, Amber Perenzin Askey, et al. 2021. "The Philadelphia Predictive Policing Experiment." *Journal of Experimental Criminology* 17(1): 15–41.
- Richardson, Rashida, Jason Schultz, and Kate 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.
- Ridgeway, Greg. 2018. "Policing in the Era of Big Data." *Annual Review of Criminology* 1: 401–419.
- Schuilenburg, Marc. 2015. *The Securitization of Society: Crime, Risk, and Social Order*. New York University Press.
- Schuilenburg, Marc. 2021. *Hysteria: Crime, Media, and Politics*. Routledge.
- Schuilenburg, Marc. 2024. *Making Surveillance Public: Why You Should Be More Woke About AI and Algorithms*. Eleven.
- Schuilenburg, Marc, and Melvin 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/paado61>
- Simon, Jonathan. 1987. "The Emergence of a Risk Society: Insurance, Law, and the State." *Socialist Review* 97: 61–89.
- Simon, Jonathan. 1988. "The Ideological Effects of Actuarial Practices." *Law and Society Review* 22(4): 771–800.
- Smith, Marcus, and Seumas Miller. 2022. "The Ethical Application of Biometric Facial Recognition Technology." *AI & Society* 37: 167–175.
- Stoker, Elsbeth. 2020. "Politie kon wekenlang meelezen met geheime berichten van duizenden zware criminelen." *De Volkskrant*, July 2.
- Swaaningen, René van. 1996. "Justitie als verzekeringsmaatschappij: 'actuarial justice' in Nederland." *Justitiële verkenningen* 22(5): 80–97.

- Van Brakel, Rosamunde. 2016. "Pre-Emptive Big Data Surveillance and Its (Dis)empowering Consequences: The Case of Predictive Policing." In *Exploring the Boundaries of Big Data*, edited by Bart van der Sloot, Dennis Broeders, and Erik Schrijvers. Amsterdam University Press.
- Weber, Max. (1921/1922) 2006. *Wirtschaft und Gesellschaft*. Voltmedia GmbH.
- Wetzell, Richard F. 2000. *Inventing the Criminal. A History of German Criminology 1880–1945*. The University of North Carolina Press.
- Zedner, Lucia. 2007. "Pre-Crime and Post-Criminology?" *Theoretical Criminology* 11(2): 261–281.