DPT

Deutscher Präventionstag –
der Jahreskongress seit 1995

Modernising Law Enforcement Intelligence for a Digital Society

Anno Bunnik

From: Claudia Heinzelmann and Erich Marks (Eds.):
International Perspectives of Crime Prevention 12
Contributions from the 13th Annual International Forum 2019 and 14th Annual International Forum 2021
within the German Prevention Congress
Forum Verlag Godesberg GmbH 2023

978.3.96410.032.0 (Printausgabe)
978.3.96410.033.7 (eBook)

Anno Bunnik

Modernising Law Enforcement Intelligence for a Digital Society

1. Introduction

The exponential rise in data and digitalisation in recent years presents a 'double-edged sword' for law enforcement agencies (LEAs). It involves huge challenges including a greater sophistication in cyber-crime, the rise of the dark web and the exploitation of the Internet for terrorist purposes. However, the data revolution also facilitates new ways of 'doing intelligence'. Big Data are increasingly mobilised for crime prevention, crime prediction and national security. A popular approach is predictive policing, developed in the United States and in recent years has increasingly been employed in Europe. In addition, Big Data and related developments such as Artificial Intelligence (AI) open manifold opportunities for data analytics and intelligence analysis. However, increasing public scrutiny puts LEAs under strong public and political pressure to mobilise Big Data and AI in an efficient, effective and ethical manner. How do state agencies strategize and operate under these constraints?

This article explores the transition of law enforcement to a digital environment. It explains how LEAs are eager to utilise Big Data but struggle to innovate successfully in this space. A case study of the United Kingdom (U.K.) highlights that senior professionals tend to be 'wooed' by new technologies and primarily direct their hope on acquiring new technology from the private sector, with limited success. Instead, LEAs would do well to invest in innovate partnerships with academia, civil society groups and other stakeholders to develop new ways of doing policing and intelligence in a networked approach.

2. The mobilisation of Big Data for policing

Whilst there is no universal definition of Big Data it can roughly be understood as the aggregation and analysis of vast datasets that capture personal information of citizens and consumers. These datasets are increasingly recognised as a viable source for a variety of purposes, primarily by the business sector (Manyika 2011; Mayer-Schönberger and Cukier 2013). The transformative potential of technology on society, however, is not a recent phenomenon. Sociologist William Ogburn coined the phrase 'cultural lag' to describe the period of time during which society needs to catch up with emerging technology (Marshall 1999; Ogburn 1922). Historical examples include wide-spread fear of trains in the nineteenth century with people being afraid that it would lead to an increase in brain diseases. Nearly a century after Ogburn first laid down his thesis on technology it is becoming increasingly clear that the pace of change is accelerating (Schmidt and Cohen 2014) primarily due to the growth of computing power, storage capacities and 'clever' algorithms that can analyse large quantities of information (Mayer-Schönberger and Cukier 2013). A case study of how state actors are dealing with this changing landscape and related societal friction in what the author calls a 'policy vacuum' (i.e., technological developments outpacing law and policy) is therefore a timely exercise.

The shift to the use of Big Data for national security and law enforcement purposes raises ontological questions on the nature of state-society relations (Mulqueen 2016). The mass usage of citizens' data by state agencies against their knowledge or consent has the potential to undermine public trust in the state. Some scholars have argued that Big Data erodes the distinction between state and civil society and between public and private domains, as state agencies "…penetrate deeply into the everyday world of civil society and private life" (Bauman et al. 2014, p. 136). Others take this argument even further adding that proactive and predictive security measures are "…meant to expand the regulatory power of governmental authorities over 'deviant' minds" (Den Boer & van Buuren 2010, p. 231). As such, these developments could seriously harm the legitimacy of governments and state institutions and negatively impact the notion of 'public consent', which is at the core of law enforcement.

This argument is perhaps further clarified with reference to the concept of 'structuration' (Giddens 1984). In a digital age, state agencies rely on access to personal data of citizens to provide the safety and security of those citizens. This mutual dependency between state agencies and citizens to provide security is primarily held together by Big Data. In this conceptualisation, data could be argued to be the energy source that powers this modern social system to deliver safety and security. Growing resistance against the use of data by the state could fracture the social system that provides security. Modern policing in the U.K. builds on the principles of Sir Robert Peel which dictates that "[t]he ability of the police to perform their duties is dependent upon public approval of police actions" (Association of Chief Police Officers 2012, p. 2). The potential erosion of public support and legitimacy makes the case for studying the role of ethics in security and law enforcement matters more pertinent. In this changing environment LEAs face several, interrelated challenges or pressures:

- *Innovation:* The exponential rise of data urges LEAs to invest in new approaches and technologies. The rationale for investment in this space is often framed in terms of effectiveness and efficiency ("better value for money''). Another reason to innovate in the digital space is to remain relevant. If police forces would ignore Social Media, for instance, it is likely that other actors will take on a policing role in the digital domain, risking the rise of online vigilantism.
- *The other side of the coin, ethics:* Since the Edward Snowden global surveillance revelations in 2013, there is emerging evidence that governments are under increasing pressure from the public, media, and civil society organisations to reconcile data-driven innovation with liberal values, such as privacy, transparency, and accountability (Lyon 2014; Bauman et al. 2014). This has led to a stronger awareness on the importance of ethics, including for law enforcement (Lyon 2014; Zwitter 2014). A holistic approach to ethics would do well to include related social and legal concerns. The social, ethical and legal implications of data-driven innovation by LEAs are pertinent and deserve to be integrated into the design of new technologies, instead of being invoked only when assessing the use of new technologies.

- *And organisational adaptation and change:* A final notion that deserves attention is organisational change. LEAs tend to be hierarchical organisations with a deeply embedded 'cop culture'. But what this means in practice is that LEAs often struggle to adapt to a new reality of rapid digitalisation and the opportunities and treats. Exploring organisational change through the prism of institutionalism allows for an interrogation of how large organisations evolve over time and what aspects of organisations facilitate and hinder change.

3. Case study: law enforcement in the U.K.

For various reasons, law enforcement in the U.K. is an exciting case study to explore the transition of this sector to a more digital society. What stands out is that the landscape in the U.K. is splintered with 45 territorial police forces, some operating in a very distinct political context, such as the Police Service of Northern Ireland (PSNI). In addition, there are various national agencies that are increasingly investing in this realm. The National Crime Agency (NCA), dubbed the U.K.'s own FBI, is a key actor when it comes to the mobilisation of data and intelligence. It is obvious that it will be a vast challenge for all these agencies to collaborate in a sustainable fashion. The sharing of data and intelligence is the first hurdle to be conquered – let alone effective cooperation in a world where crime is less territorial than it used to be.

The U.K.'s experience with intelligence-led policing (ILP) perhaps gives the country a head start compared to LEAs in several other Western countries, which have less experience in data gathering and analysis. ILP was developed here in the 1990s following experimental work by Kent Police. Over two decades of expertise in this domain has created (some) institutional capacity on intelligence gathering and analysis. However, there are still serious issues to be overcome regarding the lack of data sharing between agencies and the miscommunication between intelligence analysts and police officers in agencies (Cope 2004). What further complicates matters is that policing in the U.K. in recent years faced serious austerity measures – with some forces having to implement budget cuts as high as twenty per cent, resulting in a loss of staff, expertise and less means to invest in technological innovation. In addition, the negative consequences of Brexit on

cross-border security cooperation and the effects of the global COVID-19 pandemic places further stress on a sector struggling with a transition to a digital society.

3.1 Innovation

Law enforcement agencies face increasing pressures to take advantage of the rise of data and digitalisation. Innovation is not a new concern for law enforcement as it has always sought to catch up with the latest crime and technology developments. Cars, mobile phones, the Internet or even drones can be used both by criminals and LEAs. Digitalisation is arguably one of the most prominent frontiers in this effort, as it has facilitated new types of crime as well as crime prevention. Concerning Big Data, the premise is that this domain is perhaps easier to exploit by large organisations – which already have access to vast amounts of data – than by criminals. This competitive advantage provides manifold opportunities for law enforcement agencies to be more proactive and prevent crime before it occurs instead of responding to it (Mulqueen 2016; Stanier 2016).

The first observation is that LEAs in the U.K. are keen to mobilise Big Data. All the senior officers interviewed in this research project were highly interested in this topic and are keen to utilise data to make their organisations more effective and efficient. Secondly, Big Data allows for sharing of data, information, and intelligence between agencies. Digitalisation then drives forward the agenda of multi-agency partnerships on specific crime issues. The multi-agency safeguarding hubs (MASH) is a good example, which brings together partners around safeguarding vulnerable children. This trend will likely continue in the coming years and result in further integration of law enforcement with other public sector actors to form networked governance on 'preventative governance' strategies.

A pertinent question that this development raises is whether the sharing of data in a multi-agency partnership will also lead to the creation of new knowledge. The creation of new knowledge in a networked setting is potentially where innovation can occur. Sharing knowledge in the form of information or an intelligence product is the first step. The next would be to come to the co-creation of knowledge at the interstices of disciplines and sectors.

This research concludes that LEAs would do well to use the 'data revolution' not just to focus on the prevention of future crimes through Predictive Policing (PP) programmes, but also use it to better understand the causes and drivers of crime (Bunnik 2016). Certainly, LEAs need to attract data analysts and information workers, but should also engage the Social Sciences and Humanities (SSH) to contextualise the products of data and understand its limitations.

3.2 Ethics

New technologies employed by LEAs and national security agencies face the pressure to keep society secure as well as protect privacy. These technologies therefore face the problem of 'moral overload' having to adhere to, sometimes conflicting, value requirements (Van den Hoven, Lokhorst & Van de Poel 2012). Whilst these two values are often invoked in the public debate on Big Data it is my contention that an inclusive debate looks beyond the privacy vs. security dichotomy. Instead, there are a wide range of values involved when it comes to the mass mobilisation of Big Data. The transition to algorithmic decision-making raises pertinent questions on transparency, accountability, fairness, inclusion and other human values. The wide range of values at play certainly deserve more attention by both LEAs and academics. Moreover, taking a values-based approach to ethics begs the question: how can these values be integrated in the design of these technologies?

Senior LEA officers and staff repeatedly informed the author that their organisations need to engage more with the public to explain how Big Data is mobilised by LEAs and why this necessary. However, there is currently no coherent strategy in place how this public engagement should look like and who should take part in this dialogue. Is this a task for politicians and the regional Police and Crime Commissioner, an elected position in the U.K., or should senior LEA professionals reach out to the public to engage groups and communities on how they work with data? This engagement can take various forms, such as taking part in public seminars or appearing on talk shows on TV and radio. Currently, this happens on an ad-hoc basis with little strategy in place how this dialogue could be best approached and who should take part in it.

3.3 Organisational change

One of the first conclusions of this research project is that organisational change is largely event driven instead of data- or technology driven. A good example here are the Soham murders in 2002 that led to the creation of a national system, the Police National Database (PND). A political crisis was needed to push the sector to develop a national system. More recently, the 2011 England riots proved a game changer for LEAs as this high impact event created awareness on the role of Social Media. Many of the rioters planned the ransacking of stores on Blackberry Messenger and other apps and this spurred LEAs to better monitor these platforms for evidence in court as well as prevention of future disturbances. These historical examples elucidate that high-impact events are the primary drivers for LEAs to adopt data-driven approaches. It is perhaps no surprise that most of the officers interviewed in this research project were remarkedly critical of their own organisations regarding data and digitalisation.

In addition, this research project encountered a widespread frustration in the sector on the lack of leadership and the lack of sufficient resources to invest in the development of Big Data. Furthermore, senior officers informed the author that LEAs are often not open to change due to a deeply embedded hierarchical culture, a lack of diversity in their workforce and the lack of evidence-based review mechanisms. New skills tailored to digitalisation need to be recruited and this is now slowly taking place in various LEAs. Several agencies, such as the previously mentioned NCA, the Metropolitan Police (MPS), West Midlands Police (WMP) and Durham Constabulary are certainly ahead of others in this space and have the potential to spur change on a national level. Adaptation of dozens of agencies, however, is still mostly ad hoc and often lacks a national strategy. Both in the formal and informal domain of law enforcement, change is taking place, but this is currently insufficient to reap the full benefits of Big Data.

4. Conclusions and way forward

This review of the mobilisation of Big Data by law enforcement revealed a sector struggling with a transition to a digital society. Big Data allows for sharing of data, information, and intelligence between agencies and some multi-agency partnerships are beginning to take place, such as the safeguarding hubs. Big Data will

likely continue to drive forward these partnerships in which various agencies share their data to develop a collaborative and preventative approach to a certain problem such as vulnerable children. The real test in the coming years is if these agencies can overcome the silo mentality and develop shared intelligence and knowledge products at the interstices of their expertise. Networked innovation is slowly getting the attention it deserves as a viable alternative to purchasing new tools off the shelf. Various hurdles have to be taken, often related to institutional issues such as a strong cop culture which can resist change. Thus far, most organisational changes have been the result of high-impact events, which placed LEAs under political pressure to make better use of data.

The challenge for the coming years will be to synthesise the three above-mentioned domains of innovation, ethics, and organisational change. What are the key ingredients for an innovative institution? And how about an ethical institution? Moreover, how do we integrate ethics in the innovation processes of an organisation? With the high pace of technological change, with often unforeseen and unintended consequences, ethical reviews need to be part of the design process instead of sprinkled over the finished product at the end (sometimes referred to as 'window-dressing' or 'ethics washing'). Instead, ethics must be integrated in the design of new technological systems, toolkits, procedures etc., to ensure LEAs are not building a Kafkaesque surveillance state. This brings us to the design thinking approach. The author has recently joined the Cutting Crime Impact consortium, with six European LEAs and various academic and consultancy partners. The approach employed here is called 'human-centred design'. When we combine this with key lessons from the literature on networked innovation this could provide some cues to a sustainable way forward. Networked innovation on emerging technologies that addresses the societal, ethical and legal implications in the early stages of the design process holds the premise to deliver sustainable outcomes. As such, ethics is not necessarily a brake on innovation but instead contributes to a more robust innovation process for the greater good.

This research was supported by a grant from the European Commission: Cutting Crime Impact – Practice-based innovation in preventing, investigating and mitigating high-impact petty crime. Grant agreement ID: 787100

5. References

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D. and Walker, R. (2014) ‚After Snowden: Rethinking the Impact of Surveillance', International Political Sociology, Vol. 8, No. 2, pp. 121-144.

Bunnik, A. (2016) 'Countering and Understanding Terrorism, Extremism, and Radicalisation in a Big Data Age', in A. Bunnik, A. Cawley, M. Mulqueen & A. Zwitter (eds), Big Data Challenges: Society, Security, Innovation and Ethics, London: Palgrave Macmillan, pp. 85-96.

Cope, N. (2004) 'Intelligence led policing or policing led intelligence', British Journal of Criminology, Vol. 44, No. 2, pp. 188-203.

Den Boer, M. and Van Buuren, G.M. (2010) 'Surveillance Assemblages: Preventing Crime and Terrorism Through Data Monitoring' in Blad, J., Hildebrandt, M., Rozemond, K., Schuilenburg, M. and Van Calster, P. (eds.), Governing Security under the Rule of Law?, The Hague: Eleven International Publishers, pp. 215-234.

Giddens, A. (1984). The constitution of society: Outline of the theory of structuration. Univ of California Press.

Gstrein, O. J., Bunnik, A., & Zwitter, A. (2019). Ethical, Legal and Social Challenges of Predictive Policing. Católica Law Review, 3(3), pp. 77-98.

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. Big data & society, 1(2), 2053951714541861.

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C. and A. Byers (2011) Big data: The next frontier for innovation, competition, and productivity. Sydney: McKinsey Global Institute

Marshall, K. P. (1999) 'Has Technology Introduced New Ethical Problems?', Journal of Business Ethics, Vol. 19, No. 1, pp. 81-90.

Mayer-Schönberger, V. and Cukier, K. (2013) Big Data: A Revolution That Will Transform How We Live, Work, and Think, New York: Houghton Mifflin Harcourt.

Mulqueen, M. (2016). 'Sustainable Innovation: Placing Ethics at the Core of Security in a Big Data Age', in A. Bunnik, A. Cawley, M. Mulqueen & A. Zwitter (eds), Big Data Challenges: Society, Security, Innovation and Ethics, London: Palgrave Macmillan, pp. 61-71.

Ogburn, W. F. (1922) Social Change with respect to Cultural and Original Nature, New York: B.W. Huebsch.
Schmidt, E., & Cohen, J. (2014). The new digital age: Transforming nations, businesses, and our lives. Vintage.
Stanier, I. (2016) 'Enhancing Intelligence-Led Policing: Law Enforcement's Big Data Revolution', in A. Bunnik, A. Cawley, M. Mulqueen & A. Zwitter (eds), Big Data Challenges: Society, Security, Innovation and Ethics, London: Palgrave Macmillan, pp. 97-113.
The Association of Chief Police Officers (2012) 'Policing in the UK: A Brief Guide', [online], 23 Oct, available at http://www.acpo.police.uk/documents/reports/2012/201210PolicingintheUKFinal.pdf
Van den Hoven, J., G.-J. Lokhorst, and I. van de Poel (2012) 'Engineering and the Problem of Moral Overload', Science and Engineering Ethics, Vol. 18, No. 1, pp. 143–155.
Zwitter, A. (2014) 'Big Data Ethics', Big Data & Society, Vol. 1, No. 2

International Perspectives of Crime Prevention 12
Contributions from the 13th Annual International Forum 2019 and 14th Annual International Forum 2021 within the German Prevention Congress
Forum Verlag Godesberg GmbH 2023

Content

Introduction 7

I. Lectures and Documents from the 13th Annual International Forum

Erich Marks
Prevention Policy in a Democratic State governed by the Rule of Law Must not be Left to Soapbox Rhetoric and Populism 13

German Prevention Congress and Congress Partners
The Berlin Declaration of the 24th German Prevention Congress 31

Petra Guder, Bernd-Rüdeger Sonnen
The Transatlantic Dialogue:
US Juvenile Justice Reform at First Hand 45

Guido A. DeAngelis
The Crossover Youth Practice Model: Delivering Successful Outcomes for the Juvenile Population 57

Anthony Capizzi
Helping Juvenile Treatment Court Improve Efficiency and Outcomes with IBM's Watson Health Solution 67

Anno Bunnik
Modernising Law Enforcement Intelligence for a Digital Society 75

Miriam K. Damrow
Incongruous demands – inside child protection and education 85

Triantafyllos Karatrantos, Despoina Limniotakis
Management of Violence in Divided Societies:
Prevention of Violent Extremism and Strengthening of Democratic Principles 95

Kim Thomas, Roegchanda Pascoe
Being Resilient. Learning from Community Responses to Gangs in Cape Town: Reflections from a Manenberg activist 109

Alexander Siedschlag
A Culture of Preparedness: Fostering Prevention and Values 127

Minakshi Sinha
Transnational Organised Crime: Challenges to Criminal Justice Functionaries 135

Irvin Waller
Science and Secrets of Ending Violent Crime: What Actions will Reduce Violent Crime by 2030 to Achieve SDG 16.1 157

II. Lectures and Documents from the 14th Annual International Forum

Haci-Halil Uslucan
School as a place of orientation and as a place of prevention of disorientation 171

Gina Rosa Wollinger
Looking for Orientation. On the relevance of crises as a social seismograph 197

German Prevention Congress and its Congress partners
The Cologne Declaration of the 26th German Prevention Congress 231

Stijn Aerts
Family-based crime: an EUPCN toolbox on effective prevention 235

Kjell Elefalk
Local Safety Measurement System in Sweden 1998-2021 253

Noel Klima, Wim Hardyns, Lieven Pauwels, Lien Dorme, Birte Vandaele
Evaluation and mentoring of the Multi-Agency approach to violent radicalisation in Belgium, the Netherlands, and Germany 269

Rachel Locke
From Research to Action: Activating Strategies for Violence Reduction amidst COVID-19 281

Martí Navarro Regàs
Nightlife and cities. Challenges and urban governance at night – The vision of the European Forum for Urban Security 293

Alexander Siedschlag
Pandemic Preparedness from the Security Research Perspective 307

Erich Marks
Perspectives on Prevention during and after COVID-19. More Fire Protection and not just Fire Extinguishers! 323

III. Annex

Programme of the 13th Annual International Forum 329

Programme of the 14th Annual International Forum 337