Digital Data and Algorithms in Law Enforcement:
Some pointers for responsible implementation and use

Matthias Leese
Department of Humanities, Political and Social Sciences
ETH Zurich[1]

Abstract
Digital data and algorithms have over the past years increasingly found their way into law enforcement contexts, including modes of biometric identification and matching, automated surveillance capacities, short-term situational predictions, AI-supported analysis for large amounts of data, and the interoperability of large-scale databases and platforms for data exchange and investigation. These tools can help to increase the effectiveness and efficiency of law enforcement operations on the strategic, tactical, and operational level. They do, however, also come with a number of concerns that must be acknowledged and addressed in order to realize their potential and avoid unintended side-effects and societal frictions. Based on a multi-year research project on predictive policing in Germany and Switzerland, this paper provides a perspective on some of the challenges involved in implementing new and emerging technologies in law enforcement contexts. Specifically, it addresses (1) the nature of data, i.e. how data are socially constructed and present a particular account of the world, inevitably leading to "biased" results; (2) transparency in algorithms and AI, i.e. how "black boxes" undercut human capacities to understand and retrace processes and create problems for public accountability; (3) automation and human control, i.e. the question how human operators can retain meaningful influence over analytical processes; (4) decision-making processes and automation bias, i.e. how humans can be empowered to critically question and override system recommendations; and (5) strategic and societal implications, i.e. the fact that digital tools should not be misused to displace larger programs that address the root causes of crime.

Keywords: digitization; data; algorithms; implementation; civil liberties; accountability; police

Introduction

Digital data and algorithmic tools for their processing have over the past decade found their way into law enforcement contexts in multiple ways, including modes of biometric identification and matching, enhanced surveillance capacities, short-term situational predictions, AI-supported analysis for large amounts of data, and the interoperability of large-scale databases and platforms for data exchange and investigation. These tools can help to increase the effectiveness and efficiency of law enforcement operations on the strategic,

1 Author's email: mleese@ethz.ch

tactical, and operational level. They do, however, also come with a number of concerns that must be acknowledged and addressed in order to realize their potential and avoid unintended side-effects and societal frictions. Civil society organizations have for example warned of chilling effects of surveillance technologies, increased or new forms of data-driven discrimination, and the lack of transparency and democratic control in algorithmic decision-making (Ferguson, 2017; Robinson & Koepke, 2016; Susser, 2021).

Vis-à-vis these concerns, the challenge for law enforcement organizations is to find responsible ways of implementing and using digital data and algorithms, such that they enable enhanced strategic, tactical, and operational capacities while at the same time protecting democratic rules, civil liberties, and human rights. Law enforcement occupies a key role in society due to its mandate to produce and maintain public order. Needless to say, policing is therefore accompanied by considerable legal and moral responsibilities towards society. Crucially, the ways in which police agencies carry out their mandate undergo profound transformations when knowledge and action are based on data and pre-configured by algorithmic forms of data analysis. To think about responsible forms of digitization in law enforcement, this paper proposes five key pointers that should be given attention when implementing and using data-driven and algorithmically mediated technologies. These pointers concern (1) the nature of data themselves, as well as questions of (2) transparency, (3) automation and human control, (4) decision-making, and finally (5) strategic implications.

While these themes generally pertain to any form of the use of data and algorithms in law enforcement, they will be throughout this paper illustrated with examples from a multi-year study on the implementation and use of predictive policing software in Germany and Switzerland (Egbert & Leese 2021). During the research, empirical data on new, algorithmically mediated forms of crime data analysis for crime prevention were gathered through interviews with involved officers and analysts, field observations, as well as extensive document analysis. In total, research covered 12 police departments at the local and state level. Throughout the research period, most of the involved departments used the commercial predictive policing software PRECOBS by German manufacturer IfmPt.[1] PRECOBS specifically focuses on residential burglary and professionalized serial burglary activities, aiming to identify patterns of ongoing criminal behavior through continuous analysis of current crime data and producing risk estimates for particularly vulnerable areas or neighborhoods. In this way, it seeks to provide police departments with timely and flexible response capacities, most notably the opportunity to adjust crime prevention schemes and reallocate otherwise randomized patrols and other resources to identified risk areas in a targeted fashion. The optimal outcome of predictive policing would in this sense be to instill situational awareness that leads to the deterrence of crime (Balogh 2016; Schweer 2015).

Overall, the research project explored how predictive policing software was implemented into everyday crime analysis and crime prevention/patrolling contexts. Questions informing the research pertained to, among other things, technologically mediated knowledge production and communication within police organizations, the visualization and actionability of crime forecasts in patrolling and crime prevention, and the normative implications of policing based on data-driven risk estimates. The findings presented in this paper are based on a set of practical recommendations for the responsible use of data and algorithms in law enforcement that have been derived from the analysis of the empirical data (Egbert & Leese, 2021; Leese, 2020). They should be understood as points to consider when thinking about what data and algorithms (can) do and how they can be implemented and used in ways that speak to the particular mandate and responsibilities of law enforcement within society.

(1) Data

Predictive policing, as most other new technological tools for the purpose of intelligence and decision-making in law enforcement, is predicated upon data. The production and use of data about crime and crime fighting in law enforcement is, needless to say, not a new phenomenon (Maguire, 2012). However, with the increasingly easy production and availability of large amounts of digital data, novel insights about crime and its social contexts can be crafted from those data and inform law enforcement activities in new and more efficient ways. From an operational point of view, predictive policing rests on the assumption that crime

1 Some involved police departments did, during the research period, use different predictive policing tools that they had developed in-house. Those were, however, similar to PRECOBS with regard to the operational focus on residential burglary, theoretical and conceptual assumptions, as well as data input.

analysis – hitherto carried out manually by specialized analysts – can be algorithmically enhanced in terms of both scale and speed, enabling police departments to discover patterns of criminal activity in time to intervene into still ongoing offenses or serial crime. As a consequence, the timely availability of high-quality data as an input for pattern-detection algorithms is considered a key prerequisite for the estimation of – and intervention into – potential future crime.

Crime data are, however, rather notorious when it comes to accuracy, completeness, and timeliness (Maguire & McVie, 2017). Per definition, there is usually some lack of information about the characteristics of criminal offenses. In the case of residential burglary, initial data created from the crime scene might not yet contain complete information about stolen goods, the ways in which perpetrators gained access to a dwelling, or the time of the offense. Additionally, data creation is prone to error. Evidence at the crime scene might be overlooked, data might be entered sloppily into the database in the late hours of a night shift, or they might accidentally end up in the wrong category (Huey et al., 2021). These variables are, however, important for algorithmic pattern detection that screens for indications of professional serial burglary behavior that would make follow-up offenses likely (Townsley et al., 2003). To amend shortcomings in crime data and render them fit for analysis, there are usually multiple layers of quality control in place that check for inconsistencies such as syntactic errors or missing values (Leese, 2022). Moreover, the availability of information about criminal offences is likely to change throughout an investigation, which is why data need to be updated regularly. In summary, considerable efforts are required to render crime data trustworthy in the first place.

But apart from these practical considerations about the informational value of crime data, there are also some more fundamental concerns about the nature of data that need to be kept in mind when implementing data-driven tools for law enforcement. Data are often believed to be a true and objective representation of the world (Kitchin, 2014). As a consequence from this assumption, it is furthermore believed that if only enough data points were available, new insights about the world could be gained and the future could be modified according to specific preferences (Anderson, 2008). Data do, however, not exist independent of their creation contexts and the technical tools and practices used to produce them (Bowker & Star, 1999). When police officers produce burglary data from a crime scene, for example, they look for specific things that will allow them to describe their findings and fit them into the classification systems that structure police databases. Classification systems are relevant for the statistical processing of data, and as such a key consideration for predictive policing and other forms of crime analysis. As they already pre-structure how crime is recorded, other observations will be discarded and will not end up as analyzable crime data (Harper, 1991). Data must thus always be understood as a partial and filtered account of the world that has been constructed within a particular context and for a particular purpose (Gitelman, 2013).

This means that there is selection bias at work when data about crime and society are created. Such bias is a natural and inevitable part of any dataset and can by definition never fully be removed (Barocas & Selbst, 2016). While this means that bias must to a certain extent simply be accepted, it also means that the limitations of data must be acknowledged and interventions based on data analysis must be put into context. Law enforcement organizations should be mindful that every dataset contains over- and/or underrepresentations of certain empirical phenomena and is in its structure and informational value determined by various technical and social aspects. Importantly, as data are used as input for analytical tools such as predictive policing software, there is a danger that data bias will be perpetuated throughout the analysis and live on in the form of, for example, biased risk estimates (Kaufmann et al., 2019). Data can be a valuable resource for effective and efficient law enforcement in complex and fast-paced environments. However, their social constructedness must be kept in mind when evaluating the 'truthfulness' of data and their representative value. A healthy degree of skepticism toward their objectivity and truthfulness is appropriate, especially when they are acquired from external sources and little is known about the ways in which they were brought into being.

(2) Transparency

Algorithms range on a scale from simple and easily understandable to inherently complex and irretraceable – even for experts and programmers. Usually, the more complex variants are also the more powerful ones, as they are capable of handling large and heterogeneous datasets or even of 'learning' and adapting to new pat-

terns in the analyzed data. But even in comparatively simple and straightforward cases such as predictive policing focused on residential burglary, it can be difficult to understand how exactly crime risk has been computed and how a particular recommendation for action (e.g., "preferentially patrol this specific neighborhood within the next 48 hours") comes into being. The inner workings of complex algorithms are often called 'black boxes', meaning that humans can see the data input and the analytical output, but they can no longer understand the processes that took place in between (Latour, 1999). The likelihood of algorithms becoming black boxes further increases when commercial tools are used, as their design and analytical models are usually considered trade secrets (Pasquale, 2015). In the context of law enforcement, black boxes can have two fundamental implications.

First, they undermine institutional accountability capacities towards the public. Accountability depends on the ability to explain how decisions were made and why specific actions were carried out (Bovens, 2005). When the ways in which data are analyzed are incomprehensible for decision makers, this ability is essentially lost (Bennett Moses & Chan, 2018). A lack of accountability capacities is problematic due to the role of the police in the production and maintenance of social order. Police forces have several exceptional competencies, including the use of force and the interference with individual privacy and intimacy. Such interventions must be carefully justified in terms of their necessity and proportionate nature, which in turn requires the ability to explicate on which knowledge base they have been carried out. In fact, research indicates that police departments are increasingly turning away from the use of commercial predictive policing software and instead focus on the in-house development of predictive policing capacities – with understandability and transparency being cited as major reasons for this development (Leese, forthcoming).

Secondly, black boxes make internal resistance against data-driven analytics more likely. Research has shown that police officers and the larger organizational cultures within which they work are often skeptical towards new technologies in the first place (Manning, 1992). Such skepticism can easily turn into outright resistance when officers come under the impression that their own expertise and professional experience are threatened to be overruled by a technological tool that they cannot understand (Chan et al., 2022). As a consequence, there is a chance that recommendations for action will not be implemented on the ground (Sandhu and Fussey, 2021). In the case of predictive policing, patrol officers have, for example, shown reluctance to actually prioritize risk areas that have been identified through algorithmic crime data analysis. Such reluctance was based on the assertion that they would have better knowledge of their city/neighborhood and the crime risks associated with it than a machine.

In order to align technological capacities with external and internal transparency requirements, law enforcement organizations should thus be mindful that digital tools should always remain as transparent and comprehensible as possible, independent of whether they are commercial products or in-house developments. This will strengthen both the capacity for external accountability and the likelihood of internal compliance.

(3) Automation and control

Predictive policing software and other data-driven analytical tools automate many of the analytical tasks that previously were carried out manually by a human analyst (Perry et al., 2013). In this way, so the general idea, intelligence can be produced much quicker, on a larger scale, and without random error. Automation is thus fundamental for the advantages that data-driven analytics bring for police work. Automation does, however, come with a number of challenges. While the initial hypothesis in engineering and design for human-computer interaction was to implement as much automation as possible to free up human capacities for other, more meaningful tasks, research has over the years shown that too much automation can be detrimental for human capacities and for effective human control of activities outsourced to machines or computer systems (Parasuraman & Manzey, 2010). Moreover, it has been argued that in domain contexts where errors can have wide-ranging consequences, such as for instance nuclear safety or public security provision, automation should by default be delimited (Jones, 2017). Especially this latter point is relevant for law enforcement contexts, as high levels of automation in algorithmic data analysis effectively can entirely remove the human from the process of knowledge production and leave little or no possibility for human intervention in crime analysis, for example to double-check the plausibility of system recommendations or to correct malfunctions or other errors.

In predictive policing, the automation of crime analysis processes through algorithmic means has been shown to facilitate the work of crime analysts due to its potential to relieve humans of repetitive and monotonous tasks. At the same time, police departments have emphasized the need to subject automation to rigid human control in the form of an operator who is set up to be "in the loop". Keeping a human in the loop requires a system to interrupt automated processes at pre-defined points and only to continue when active approval is given by the user. In this way, human awareness of analytical functions carried out by the software is ensured and a possibility to double-check input data and the plausibility of output is granted. This is important in regard to the potential lack of trustworthiness in crime data, but also in regard to issues of bias and accountability discussed above (Cummings, 2006).

Research has shown that police departments ensure control over automated data analysis processes in several ways. Most notably, predictive policing software is exclusively executed by human operators, who in most cases are trained and experienced crime analysts. While fully automated analyses would in theory be possible, an operator is considered a necessary safeguard against faulty data input, system malfunctions, and implausible outputs. Importantly, a human operator is expected to be able to put estimates about crime risks into a larger situational picture and available resources. Other forms of safeguards consist of a four-eyes principle during the review of system output, or checklists that instruct human officers to cross off potential error sources in a systematic fashion before confirming system outputs and forwarding them to local stations for front line implementation.

Given the implications of data-driven knowledge for the ways in which society becomes policed and how resources in public security provision are re-distributed, law enforcement organizations should be mindful that, in principle, full automation of analytical processes by means of technological tools should be ruled out. It is important to carefully configure automation and human oversight in ways that ensure meaningful control at all times. To do so, human analysts must always remain in the loop and have meaningful control over system functions. That means that algorithmic systems must not withhold information from the user or proceed at critical junctions without user approval. Only then will law enforcement agencies be able to benefit from novel analytical insights while at the same time firmly remaining in the driver's seat.

(4) Decision-making

The main implication of data and algorithms in law enforcement is to aid decision-making and planning. The general idea in this context is that more effectiveness and efficiency can be accomplished if the strategic, tactical, and operational level are informed by data-driven knowledge. There is, however, a risk that algorithmically produced recommendations are uncritically followed (Cummings, 2004). The reason for this 'automation bias' is that humans consider technical systems to be objective, neutral, and immune to error. Given the potential error sources in data-driven analytics discussed above, it is, however, key that decisions about the allocation of security provision are not exclusively determined by technological tools.

In predictive policing, initial decisions about the suitability of data-driven crime risk estimates are, as discussed above, made by a human operator who is tasked with plausibility checks of system input and output. Only after human review do forecasts become part of concrete crime prevention schemes. Human review is particularly important in those cases where plausibility conditions are not fully met, for example when input data are incomplete or when identified risk areas do not align with the larger situational picture or the professional experience of operators. In such cases, it is key that humans are encouraged to overrule system recommendations in order not to implement misleading risk forecasts into crime prevention operations and waste resources instead of using them in a targeted fashion. Research has, however, shown that it can be challenging to argue against allegedly neutral and objective system outputs, particularly when counter-arguments are based on non-systematized evidence such as personal experience or a "gut feeling". Moreover, in the domain of security provision, a foundational principle is to rather err on the side of caution than to miss out on the prevention of harm. Consequently, operators tend to approve system outputs even in cases where they do not fully agree.

In order not to go against the rationale of data-driven knowledge, that is, to put resources to use in more effective and efficient ways, law enforcement organizations should thus ensure that operators are put in

a position where they can make informed and responsible decisions. To do so, they should actively be encouraged to engage with all aspects of the analytical process, including the explicit right to overturn algorithmically produced intelligence and recommendations for action. As blind trust in algorithmically produced intelligence and recommendations for action might lead to faulty operational decisions that can undercut the effectiveness of police work and deteriorate the relationship between law enforcement and the public, critical engagement with algorithmic recommendations should be encouraged and the right to override them should be facilitated and institutionally enshrined. More generally speaking, law enforcement organizations should also be mindful that human decision-making is a key assumption in both legal and moral terms, and that automated decision-making would have negative implications for questions of accountability as discussed earlier.

(5) Strategic implications

Whereas the previous themes have mostly highlighted operational quandaries in the use of data and algorithms for law enforcement purposes, there are also important strategic implications that must be considered vis-à-vis such technologies. In light of political discourse, media attention, as well as financial commitments made through procurement and implementation, there is often a perceived need to maximize the utility of predictive policing and other data-driven analytical tools (Egbert & Leese, 2021). This perceived need leads to overemployment, demonstrating to policy-makers and the general public that financial commitments are being put to good use. This can, however, in turn lead to one-dimensional problem perception and corresponding treatment.

Predictive policing tools, for example, have been designed largely on assumptions from environmental criminology and situational crime prevention. Implicitly, these approaches contend that crime is a natural part of human behavior/societal forms of organization and that it can thus be expected that crime will happen by default if not prevented or otherwise intervened into. Operationally, they therefore favor policing approaches built on deterrence by means of increased police presence, environmental modifications, and (technological) means of target hardening. This means that they aim to suppress rather than evaluate why crimes happen and how incentives for criminal behavior could be addressed in the first place (Wilson, 2018). Such a focus rules out questions concerning the root causes of crime and their possible resolution through social reform, as for example found in community policing approaches.

Admittedly, the reasons for the occurrence of crime might often be outside the scope of law enforcement activities. Nonetheless, it is important to keep in mind that technological tools can reinforce particular strategic approaches to crime control while marginalizing others. Data and algorithms should, in this sense, not be used to replace programs of community engagement and larger debates about social reform. For law enforcement organizations, this means that the capacities and limitations of new and emerging technologies must be carefully assessed. Predictive policing software can, for example, be a powerful tool for the efficient use of resources and targeted and effective crime prevention – but outside of these narrow boundaries, it offers little insight into the larger dynamics of crime and society. It should thus remain a complementary tool in the overall toolkit of the police and not be used to suppress or replace long-term strategic programs that address the root causes of crime. Law enforcement agencies should be careful not to overemphasize the role that data-driven analytics can and should play in their work.

Conclusions

This contribution has given a brief, cursory overview of some of the issues that are at stake as law enforcement agencies increasingly integrate data and algorithms into their daily work practices. As has been shown, data-driven knowledge and action reconfigure how the police go about their business and in doing so also affect the role of the police in the production and maintenance of public order and the interface between law enforcement and the general public. The pointers presented here speak to some of the most pressing questions that need to be reflected when integrating new technological tools into security work. The issues discussed here should not be regarded as exhaustive, but rather as representative of some of the most pertinent challenges that police departments faced when dealing with predictive policing software.

The pointers for the responsible use of data and algorithms can both be used as a form of reflection and as a practical guideline. Clearly, the message here is not to not use new technologies at all. On the contrary, it can hardly be denied that law enforcement agencies require updated tools to cope with new challenges in complex and fast-paced environments. The implementation and use of new tools can, however, be understood as a welcome opportunity to further align operational requirements and the protection of democratic rules, civil liberties, and human rights. In this sense, every prototype, every trial run, and every implementation process of a new technology can be seen as a chance to ensure that the use of data and algorithms will not create (unforeseen) detrimental societal effects. Paying attention to the pointers laid out throughout this contribution can serve as a starting point that puts law enforcement organizations in a position to critically assess and reflect how new and emerging technologies can be implemented and used in a responsible fashion. In the end, it should be in the interest of society not to undercut the capacities of law enforcement. But just as well, law enforcement organizations should have a strong interest to respect democratic rules, civil liberties, and human rights.

References

- Anderson, C. (2008) The End of Theory: The Data Deluge Makes the Scientific Method Obsolete. *Wired* (16.07).
- Balogh, D. A. (2016) Near Repeat-Prediction mit PRECOBS bei der Stadtpolizei Zürich. *Kriminalistik* (5):335-341.
- Barocas, S. & Selbst, A. D. (2016) Big Data's Disparate Impact. *California Law Review* 104 (3):671-732.
- Bennett Moses, L. & Chan, J. (2018) Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability. *Policing and Society* 28(7): 806-822.
- Bovens, M, (2005) Public Accountability. In Ferlie E, Lynn L E J & Pollitt C (eds.) *The Oxford Handbook of Public Management.* Oxford: Oxford University Press, 182-208.
- Bowker, G. C. & Star, S. L. (1999) *Sorting Things Out: Classification and Its Consequences.* Cambridge: MIT Press.
- Chan, J., Sanders, C., Bennett Moses, L. & Blackmore, H. (2022) Datafication and the Practice of Intelligence Production. *Big Data & Society* 9(1): 1-13.
- Cummings, M. L. (2004) Automation Bias in Intelligent Time Critical Decision Support Systems. AIAA 1st Intelligent Systems Technical Conference. Chicago, Illinois.
- Cummings, M. L. (2006) Automation and Accountability in Decision Support System Interface Design. *Journal of Technology Studies* 32(1): 23-31.
- Egbert, S. & Leese, M. (2021) *Criminal Futures: Predictive Policing and Everyday Police Work.* London/New York: Routledge.
- Ferguson, A. G. (2017) Policing Predictive Policing. *Washington University Law Review* 94(5): 1115-1194.
- Gitelman. L. (ed.) 2013. *"Raw Data" is an Oxymoron,* Cambridge: MIT Press.
- Harper, R. R. (1991) The Computer Game: Detectives, Suspects, and Technology. *British Journal of Criminology* 31(3): 292-307.
- Huey, L., Ferguson, L. & Koziarski, J. (2021) The Irrationalities of Rationality in Police Data Processes. *Policing and Society* online first: 10.1080/10439463.2021.2007245.
- Jones, M. L. (2017) The Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood. *Social Studies of Science* 47(2): 216-239.
- Kaufmann, M., Egbert, S. & Leese, M. (2019) Predictive Policing and the Politics of Patterns. *British Journal of Criminology* 59(3): 674-692.
- Kitchin, R. (2014) Big Data, New Epistemologies and Paradigm Shifts. *Big Data & Society* 1(April-June): 1-12.
- Latour, B. (1999) *Pandora's Hope: Essays on the Reality of Science Studies.* Cambridge: Harvard University Press.
- Leese, M. (2020) Predictive Policing: Proceed, but with Care. *CSS Policy Perspectives* 8 (14).
- Leese, M. (2022) Enacting Criminal Futures: Data Practices and Crime Prevention. *Policing and Society* online first: 10.1080/10439463.2022.2112192.

- Leese, M. (forthcoming) Predictive Policing and Human Rights: The Swiss Case. Amsterdam: Amnesty International.
- Maguire, M. (2012) Criminal Statistics and the Construction of Crime. In Maguire M., Morgen R. & Reiner R. (eds.) *The Oxford Handbook of Criminology*, Oxford: Oxford University Press: 206-244.
- Maguire, M. & McVie, S. (2017) Crime Data and Criminal Statistics: A Critical Reflection. In Maguire, M., Morgan, R. & Reiner, R. (eds.) *The Oxford Handbook of Criminology.* Oxford: Oxford University Press, 163-189.
- Manning, P. K. (1992) Technological Dramas and the Police: Statement and Counterstatement in Organizational Analysis. *Criminology* 30(3): 327-346.
- Parasuraman, R. & Manzey, D. H. (2010) Complacency and Bias in Human Use of Automation: An Attentional Integration. *Human Factors* 52(3): 381-410.
- Pasquale, F. (2015) *The Black Box Society: The Secret Algorithms that Control Money and Information.* Cambridge: Harvard University Press.
- Perry, W. L., McInnis, B., Price, C. C., Smith, S. C. & Hollywood, J. S. (2013) *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations.* Santa Monica: RAND Corporation.
- Robinson, D. & Koepke, L. (2016) Stuck in a Pattern: Early Evidence on "Predictive Policing" and Civil Rights. Upturn.
- Sandhu, A. & Fussey, P. (2021) The 'Uberization of Policing'? How Police Negotiate and Operationalise Predictive Policing Technology. *Policing and Society* 31(1): 66-81.
- Schweer, T. (2015) „Vor dem Täter am Tatort" - Musterbasierte Tatortvorhersagen am Beispiel des Wohnungseinbruchs. *Die Kriminalpolizei* 32 (1):13-16.
- Susser, D. (2021) Predictive Policing and the Ethics of Preemption. In Jones B. & Mendieta E. (eds.) *The Ethics of Policing: New Perspectives on Law Enforcement.* New York: New York University Press, 268-292.
- Townsley, M., Homel R. & Chaseling J. (2003) Infectious Burglaries: A Test of the Near Repeat Hypothesis. *British Journal of Criminology* 43 (3):615-633.
- Wilson, D. (2018) Algorithmic Patrol: The Futures of Predictive Policing. In Završnik A. (ed.) *Big Data, Crime and Social Control.* London/New York: Routledge, 108-127.