Digitalising law enforcement: A critical guide from the Nordic-Baltic countries and the UK

Vasileios Galis, IT University of Copenhagen, Denmark

The aim of the Critical Understanding of Predictive Policing (CUPP) project is to critically engage with the implications of new technologies and advanced data integration and analysis in relation to police work. CUPP conducts research to provide comprehensive evidence-based interdisciplinary knowledge on the various manifestations of digitalisation and prediction in law enforcement across six national contexts: Denmark, Estonia, Latvia, Norway, Sweden, and the UK. The police constitute a key institution that would benefit from digitalisation, so as to make Nordic government bureaucratic operations more efficient [1], reduce fiscal burdens [2], improve accuracy of decision-making, and streamline data management [3]. Predictive analysis of digital data is ascribed with significant potential to prevent crime in the Nordic context [4]. CUPP constitutes a comprehensive technology assessment to critically study and evaluate new police technologies as well as to inform and build public and political opinion about them. By doing so the project addresses several of the societal challenges highlighted at both the EU and Nordic level focusing on major concerns shared by citizens in the Nordic countries regarding: (i) inclusive, innovative, and reflective societies, and (ii) protecting freedom and security of the Nordic Region/Europe and its citizens.

Major challenges: digitalisation under critique

Based on our fieldwork, digitalisation challenges law enforcement in multiple ways:

Firstly, the police must *either* undertake public procurement of digital police tools, thereby outsourcing core issues of police data to private actors *OR* it must develop substantial technological competencies in-house. Our case studies have shown that outsourcing comes with significant security and privacy risks as well as a loss of control over key features of law enforcement and potential vendor lock-in for specific commercial solutions. For example, in the Norwegian context our partners showed that the value of societal trust is high, and predictive policing must not reduce trust. The development of digital policing technologies has been significantly slower in Norway because of the desire for gradual change in policing and for the safeguarding of trust. Prioritising trust led to abandoning a multimillion police digitisation project. On the other hand, in-house competence capacity-building also comes with a heavy price tag and with a risk of each police department "re-inventing the wheel". This first challenge concerns how the police can develop so as to "own" technology as part of its core: traditional professional roles must change, and technology must become part of how law enforcement is formulated, executed, and experienced.

Secondly, the CUPP project argues that when technology becomes part of the limits of law enforcement, such as how it is pre-set, pursued, and perceived, new questions emerge as to how "analogue" questions of policing – meaning physical encounters between the police and citizens – are translated into binary code. This second challenge concerns algorithmic politics [5], but also the streamlining of administration within law enforcement. CUPP investigates the implications of the digitalisation of law enforcement for the contemporary democratic polity in an era saturated with new public analytics [6]. In line with many critical voices around the datafication of police forces [7, 8, 9, 10], CUPP brings an interdisciplinary magnifying glass over emerging data technologies and organisational practices that enable the digital transformation of the police. For example, investigating the implementation of the *Status System* – a digital platform used by the Swedish police – has uncovered biased policing practices, where individuals from marginalised communities are disproportionately targeted and subjected to police scrutiny. This can lead to increased distrust between these communities and the police, potentially undermining social sustainability, and coherence.

Similarly, in the Norwegian case, concerns about the quality of data related to the life-course of young offenders in general and of youth resilience, or rather the lack of a holistic oversight of the lives of young people, produces one-dimensional portraits of young lives. This methodology/preventive technique leads to youths being viewed as a threat or danger. Our colleagues in Norway note that in this context, treating youths as a security risk implies consequences for net-widening of control. The CUPP case on the implementation of Face Recognition Technologies (FRT) in the UK showed that this new type of surveillance carries and even exacerbates to a significant extent the very same historical discriminations running through the traditionally divided and polarised UK society. In Latvia, our partners note that the development and implementation of traffic surveillance via digital means may be problematic when considered from the perspective of compliance with fundamental rights, data protection law and democratic principles of governance. In other words, CUPP argues that within this widened landscape, pre-existing inequalities are likely to be exacerbated, while transparency in policing practice can be even more challenging than it has been historically. Moreover, in all cases, several police officers expressed scepticism and reluctance to the digitalisation of their organisations. Some even talk about predictive policing as just being hype and a buzzword. All of this signifies the need for not only shedding light on the social and democratic implications of policing in the age of big data but also acknowledging the rigorous transformations of the working world of police officers through the application of data platforms.

Thirdly, the digitalisation of law enforcement affects how different police departments share data, both vertically and horizontally. Data submitted or harvested by one institution may later acquire evidential character elsewhere in the justice system, as it is interoperably shared between institutions (e.g., border police and migration authorities). Although interoperability[A] is seen as 'a technical rather than a political concept' by the European Commission [11], interoperable digital systems challenge existing structures and cooperation dynamics and also redefine the role of the actors involved in the operationalisation, process, and enforcement of the law at the intersections of executive, legislative, and judicial power [12]. In the Norwegian case, lack of effective interoperability in the developing process of the new police digital platform Omnia led to a public procurement fiasco. In the UK, live facial recognition has been predominantly linked to CCTV cameras, with police rolling out opaque trial operations in many city centres. In Denmark, there is no political/policy debate regarding how data is stored, integrated, and used in the data-driven police platform. In Latvia, the implementation of digital traffic control tools has not changed patterns in traffic behaviour. Our partners from Estonia go as far as to claim that the public is ready to accept digital policing technologies once a practice becomes common, without caring if data selection and sharing is efficient, interoperable, and constitutionally sound. Thus, one of the major recommendations that has emerged from our research work in CUPP is that **the digitalisation of the police must be treated holistically as part of an interoperable network rather than focusing on different parts of the police in isolation.**

[A] Interoperability is a characteristic of a product or system that works with other products or systems. The term was initially defined as information technology or systems engineering services that allow for information exchange. A broader definition considers social, political, and organisational factors that impact system-to-system performance [13].

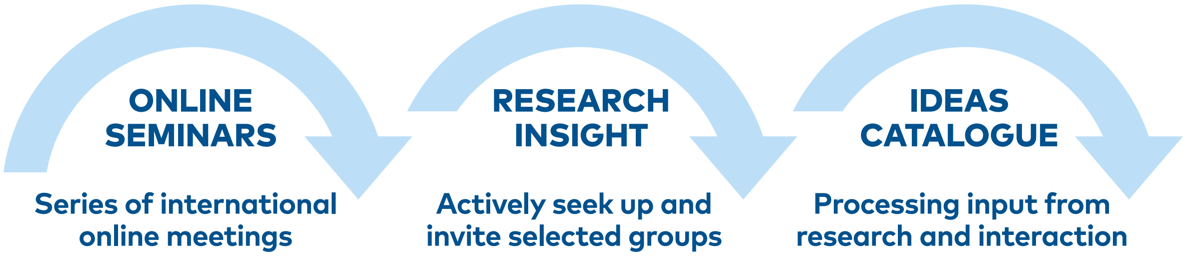
Data in the dock

Several voices, including highly ranked police officers and politicians across the countries under investigation, claim that digital or predictive policing can be a rationalising force with the potential to reduce prejudices, increase efficiency, and improve prediction accuracy. However, the use of digital technologies may technologically reify bias and deepen existing patterns of inequality [14]. As mentioned above, this has also been manifested in several of the country case studies conducted in the framework of the CUPP project: digital technologies inadvertently and unavoidably carry legacies of (post)colonial, class and gender discrimination that are maintained along in the algorithms/ontologies dictating the use of data and data platforms.

At the same time, a cautious view of technological optimism (cf. 15) is promoted by proponents of the digitalisation of the police, and the challenge is that there are clear gaps in the division of responsibilities and regulation concerning digital technologies. These solutions and perceptions of data driven police platforms are largely speculative and techno-positive. As became evident in the case studies from Estonia, people's perceptions are significantly influenced by social perceptions of data collection and sharing. For example, biometric data collection was often perceived critically, while sharing passports was considered a common normative practice. However, biometric passports are becoming increasingly common, and the Estonian public does not seem to have the same critical reaction. Based on the findings of the Estonian CUPP team, the development and presentation of data technologies play a significant role in shaping public perceptions. There is a need for political scrutiny that monitors how data driven tools are perceived, presented, adopted, and adapted in law enforcement, and critically problematizes data integration and analysis methods that lead to the criminalisation of certain populations.

In line with CUPP's research scope, this policy brief disseminates knowledge on the latest developments within data driven police practices in the region and promotes a community-based research culture that assists civil society in being able to move closer to achieving Goal 16 of the UN Sustainable Development Goals (SDGs), that is, educating people about the challenges brought about by the digital transformation of policing. CUPP's objective is to contribute to a socially sustainable Nordic region by investigating how social and cultural values, politics, and bias, are perceived, and embedded in data-driven police innovations, as well as experienced, and practiced by citizens, law makers, police officers and developers. To support continuous knowledge exchange with policy and practice in the Nordic region we have, together with PROSA, developed a critical engagement model.

Engagement Process



ONLINE SEMINARS

Series of international online meetings

- POL-INTEL (DK)
- Status (SE)
- Prejudice and algorithm bias (EST)
- Mass surveillance in traffic contr. (LV)
- Forecasting future crimes (NO)
- Facial recogn. and publ. space (UK)

RESEARCH INSIGHT

Actively seek up and invite selected groups

- Students (Soc. Data, Criminology)
- Rights groups (free legal aid)
- Professionals, wider IT community
- Commuter associations
- Amnesty International
- Twitter contacts

IDEAS CATALOGUE

Processing input from research and interaction

- Fundamental Rights
- Transparency
- Law changes
- Tools
- Visualisation

Promoting critical engagement: blowing the whistle of digital police technologies

The CUPP project allies itself with social struggles related to inequality, ethical concerns, human rights, and fundamental freedoms as well as to the various data justice, security and privacy issues raised by the digitalisation of law enforcement and their implications for democracy [16]. CUPP's interventionist approach represents an effort through research to foster knowledge and support marginalised views in relation to the deployment of predictive policing software in the countries under investigation. We do this either by:

- Hypothesising that as relations between citizens and the state are increasingly digitalised, and as private companies are now playing a significant role in developing the infrastructures that deliver policing, political action is needed to understand how transparent police institutions and innovations come into being in practice.
- Conducting research that will hold the police accountable for the justice of their actions and credibility of their analyses.
- Engaging in debate with relevant stakeholders.
- Allying with social scientific research on innovation and critical police studies to shed light on the social dimensions of policing in the age of big data.
- Investigating to what extent police data analytics is a rationalising force with the potential to reduce bias, increase efficiency, and improve prediction accuracy or even the opposite, that is reifies biases and deepens existing patterns of inequality.
- Asking how public participation, transparency, and fundamental rights are ensured in the procurement, implementation, and use of digital policing infrastructures when public and private actors collaborate within these digital infrastructures.

To conclude, CUPP encourages political action that approaches digital innovations within law enforcement in a socially consequential context. CUPP's critical engagement acts as a bridge to the larger population without specialist knowledge. We see the value of critical scrutiny on police data-driven innovations not only for policing, but also for law and regulation mechanisms, criminology, social inequality, and research on big data analytics in other public sector institutions. CUPP puts these innovations, and its democratic implications, at centre stage, and invites political action to strengthen grassroots social institutions, by increasing these groups' access to justice.

References

1. Montero J, Finger M. The rise of the New Network industries: regulating digital platforms. Routledge: 2021.
2. de Mello L, Ter-Minassian T. Digitalisation challenges and opportunities for subnational governments. 2020.
3. Gundhus HOI, Talberg N, Wathne CT. From discretion to standardization: Digitalization of the police organization. International journal of police science & management. 2022; 24(1): 27-41.
4. Jansen F. Data driven policing in the context of Europe. Data Justice Lab, 2018. Available at: https://bit.ly/2tQquMT
5. Amoore L. Machine learning political orders. Review of International Studies. 2023;49(1):20–36.
6. Yeung K. Algorithmic government: Towards a new public analytics? In: Proceedings of the ThinkBig Workshop, Windsor, UK: 2018. p. 25-26.
7. Ferguson AG. Rise of Big Data Policing, The. In: Rise of Big Data Policing. The New York University Press: 2017
8. Kaufmann M. Who connects the dots? Agents and agency in predictive policing. In: Technology and agency in international relations. Taylor & Francis: 2019.
9. van Brakel R. Rethinking predictive policing: Towards a holistic framework of democratic algorithmic surveillance. In: The Algorithmic Society. Routledge: 2020. p. 104-118.
10. Brayne S. Predict and surveil: Data, discretion, and the future of policing. Oxford University Press, USA: 2020.
11. de Hert P, Gutwirth S. Interoperability of police databases within the EU: an accountable political choice?. International Review of Law Computers & Technology. 2006;20(1-2): 21-35.
12. Galli F. Interoperable law enforcement. Cooperation challenges in the EU area of freedom, security and justice. Cooperation Challenges in the EU Area of Freedom, Security and Justice (February 2019). Robert Schuman Centre for Advanced Studies Research Paper No. RSCAS, 2019, 15.
13. Slater T. What is interoperability?. Network Centric Operations Industry Consortium-NCOIC: 2012.
14. Brayne S. Big data surveillance: The case of policing. American sociological review. 2017; 82(5): 977-1008.
15. Morozov E. To save everything, click here: technology, solutionism, and the urge to fix problems that don't exist. Allen Lane: 2013.
16. Dencik L, et al. Exploring data justice: Conceptions, applications and directions. Information, Communication & Society. 2019; 22(7): 873-881.

↩ Back to table of contents