

# NEGOTIATING DIGITAL TRACES

*The epistemic power of recorded police data*

by Helene O. I. Gundhus, Pernille Erichsen Skjervak & Christin Thea Wathne

Drawing on two empirical cases in different Norwegian police units, we explore how the increasing data gathering, recording, sorting, standardizing, and integration required by the Norwegian police's Intelligence Doctrine is experienced by users. Inspired by domestication theory, we provide new insights into police officers' varied perceptions, interpretations, and use of data. Our main finding is that digital traces were not necessarily used as the steered and managed intelligence process envisioned in the Intelligence Doctrine, and that this led to various adverse outcomes. Police officers engaged with recorded and digital traces in varied ways—rejecting, resisting, ignoring, supporting, adopting, or negotiating them. The intelligence process was constrained by bias inherent to the system, which resulted from focusing information gathering on what was already available, and from connecting it to recurrent individuals and problems. In the processes of turning analogue objects into digital ones, police officers' gut feeling and intuition still mattered, for example when information was selected for the crime intelligence system. The way the police related to the epistemic power of the data varied, but officers were obliged to relate to this uncertain element. Despite the standardized framework for how data should be applied, differences in practical routines, the digital tools used, symbolic work and learning processes revealed that its domestication in the police organization was messy. We found gaps between policy and practice, which can be seen both in unexpected workarounds and in solutions for organizing routines and everyday work. These reciprocal processes influenced and were influenced by police culture. As police intelligence evolves, the interpretation and utilization of recorded data may change, especially with the use of algorithms and artificial intelligence. Future research will show how police navigate between data-driven and observation-based narratives, and how this affects their social identity within a continuum of "datafied" and "contextual" police culture.

**Keywords:** Digital traces, domestication theory, epistemic power, intelligence-led policing, police

**Author:** Helene O. I. Gundhus,  
Professor, Department of Criminology and Sociology of Law at the University of Oslo,  
Professor II, Norwegian Police University College, Norway

Pernille Erichsen Skjervak, PhD Candidate,  
Centre for the study of Professions, Oslo Metropolitan University, Norway

Christin Thea Wathne, Research Professor,  
Work Research Institute (AFI), Oslo Metropolitan University, Norway

**Licensing:** All content in NJSTS is published under a [Creative Commons Attribution 4.0 license](#). This means that anyone is free to share (copy and redistribute the material in any medium or format) or adapt (remix, transform, and build upon the material) the material as they like, provided they give appropriate credit, provide a link to the license, and indicate if changes were made.

## Introduction

Intelligence-led policing is one of the main strategies embraced by police services in the Western world (Fyfe et al., 2018). The Norwegian police implemented a version of intelligence-led policing in 2014—to support managers' decision-making in governing and preventing crime. In the National Police Directorate's Intelligence Doctrine, intelligence-led policing is described as a management approach to how the police should collect data, analyse it, and report it to managers (National Police Directorate, 2014; 2020). Information and communication technology (ICT) is key in this work, its aim being to share and act upon data to make reliable and actionable intelligence reports. In the doctrine, making intelligence is described as a process whereby «raw» data is converted into meaningful information, which can be used to make assessments of possible future developments (Helmersen, 2024, p. 151). One aspect of this that is not clearly described is the significance of the repurposing of data, so that data collected for one purpose can be reused for other purposes: a phenomenon known as 'digital data recycling'. This recycling relies heavily on the input of officers to police registers during their everyday work, which we refer to as creating 'digital traces'. In this article we ask *how this recorded data is used, seen and integrated into the organization's everyday routines*.

Our exploration of the significance of digital data is inspired by the domestication theory developed by Lie and Sørensen (1996), which analyses how technologies are interpreted and used in three dimensions. The first of these is practical work, where users develop patterns of usage when making artifacts part of their daily routines; the second is symbolic work, where people attach symbolic meanings to artifacts and adopt or transform the meanings inscribed in the technology; the third is cognitive work, which includes learning about artifacts (see also Sørensen, 2006). This approach aims to sharpen the analytical focus on the use of technology and local negotiations, and on the way users also reshape the technologies in these three dimensions in a two-way process (Ask, 2016).

To analyse the knowledges, practices and interpretations at play in the domestication of digital data recycling we examine two empirical cases. The first involves the application of intelligence to prioritize resource allocation in local and central units within a police district we will call «South Police District» for reasons of anonymity. The second involves the application of intelligence to youth crime prevention in

a local unit in what we will call «Central Police District». Our starting point is that digital data is not objective or neutral: it is made visible through «digital prisms that 'refract' social domains and configure and reconfigure relations between datasets and algorithms in the making of actionable knowledge relating to pasts, presents and futures» (Flyverbom, 2024, p. 3). Data is imagined, selected, curated and shaped, to make social phenomena seeable, knowable and governable (Kaufmann, 2023). Information is extracted, decomposed, and needs to be condensed. This process of datafication «has consequences for its shape and the decisions we come to make based on data-based proxies that stand in for the original richness and complexity of the domain» (Flyverbom, 2024, p. 4).

In particular, we will explore how the tendency towards ever more gathering, recording, sorting, standardizing and integration of the data required by practicing intelligence-led policing is experienced by users in the organization. Digital traces lead to new visibilities, knowledge and governance in the police (Flyverbom, 2022, Lundgaard et al., 2022), and we explore how these are handled by different groups in different contexts. We are particularly interested in how different user groups acknowledge or challenges the recorded data, and by this negotiates the data's epistemic power. The term 'epistemic power' will be used to describe what are perceived as reliable and credible representations of knowledge (through storytelling, answering questions, or providing facts) which do not necessarily have any legitimate source, but which can influence what comes to be regarded as knowledge (Archer et al., 2020). Inspired by domestication theory, we provide new insights into how and why police units differ in their perception, interpretation and use of data.

The article is structured as follows: we first present the theoretical framework, the context of the digitalization of the Norwegian police, and the empirical cases and methodology. The first part of the analysis describes work routines, and the importance of digital traces and datafied information in intelligence work. We then look at differences in the understanding of digital traces in different police units, – that is, the way their practice, through collective symbolic structures, gives epistemic power to registered and visible data. Finally, we discuss how these variations in knowledges shape the learning and governing processes of police organizations.

## Theoretical framework

We take a sociotechnical approach to user experiences, to which the domestication theory is relevant, since it approaches technologies from the user's point of view (Ask and Søraa, 2024, p. 65-67). The theory evolved out of media studies interest in how audiences listened to or viewed different types of media (Haddon, 2007). The Social Construction of Technology (SCOT)-approach, holds that

rather than human actions being determined by technology, human action shapes technology, and makes the user central: users matter in the construction of technologies for instance, they demand that bikes should be made safe. In their definition of SCOT, Pinch and Bijker (1984) saw users as playing a key part in technological change (see Oudshoorn & Pinch, 2007).

The word 'domestication' conveys how new technologies are transformed from being 'wild', unfamiliar, exciting, and possibly threatening into familiar objects embedded in the culture of society and in the routines of everyday life (Silverstone et al., 1992; Lie & Sørensen, 1996). Silverstone and Haddon looked at how computers were introduced into the home and «tamed» by being used in a familiar setting (Silverstone & Haddon, 1996). More recently, domestication has been viewed as a two-way process in which both technological objects and people may change (Oudshoorn & Pinch, 2007), so that it can be described as a co-production between humans and technology, with both parties being modified in a two-way process (Ask, 2016, p. 16). For STS studies, co-production of the social and the technical dimension is fundamental (Ask, 2016, p. 66; Jasanoff, 2004; Sørensen et al., 2000). In this article we will therefore interpret knowledge transfer in a non-linear way, with knowledge taken from the data system by police officers being regarded as co-production.

Although we argue that this is a two-way process, our main focus will be on police officers' interpretation and use of data from ICT systems: it is their perceptions and interpretation of it that will be in the foreground. Due to the co-production of the data, the materiality of the technology will also shape officers' perceptions. However, we are not conducting an analysis of the functionality, design and related symbols and stories of the technologies, (what Ask and Søraa (2024, p. 85) call a script analysis), users will be the focus of our attention.

Selwyn and Cumbo (2024) claim that all domestication studies identify four stages of technology in institutional settings:

- (i) 'Appropriation': the acquisition of the technology and its initial incorporation into institutional spaces and practices;
- (ii) 'Objectification': the location and arrangement of the technology within the material, social, and cultural spaces of the institution;
- (iii) 'Incorporation': the integration of technological practices into the daily routines of institutional life and the change of capabilities that results;
- (iv) 'Conversion': the integration of the technology into people's self-identities and the broader social relations between the institution and the outside world (Selwyn & Cumbo, 2024, p. 91).

As early as the nineties, researchers at the Norwegian University of Science and Technology suggested that it is more fruitful to see domestication as composed of dimensions rather than stages (Ask, 2016). This is particularly true in the case of ICT, since it is difficult to separate the user from the producer of the outcome (Ask, 2016). In this Trondheim model, domestication includes the symbolic, practical, and cognitive work mentioned in the introduction. Although we are not conducting a traditional domestication analysis conforming to the theory (see Ask & Søraa, 2024), we take inspiration from this approach, and will explore practical, interpretative and learning aspects of digital traces in the two cases of police work.

In the analysis we will use three theoretically informed concepts to examine these dimensions: datafication, digital traces and epistemic power. 'Datafication', is used to describe domestication practices whereby human actions and proxies for it, are categorized and turned into searchable data in a database. Datafication is closely associated with management, control, and prediction (Flyverbom, 2022). What is seen and known is used to govern the present and the future. According to the Police Intelligence Doctrine, intelligence must be used to improve predictions. The digital prism, or what Beer (2019, in Flyverbom, 2022, p. 4) terms 'the data gaze', creates a particular form of visualization and knowledge production. As argued by Flyverbom, «Patterns or predictions are always to some degree 'proxies' for a given object (Mulvin, 2021), and the distance between the two is important to account for, as also suggested by Tsoukas (1997) in his work on 'information reductionism'» (2024, p. 7).

Digital traces, the second concept, are central to digital data recycling, where data collected for one purpose can be reused for others. Digital traces left on digital platforms are therefore of value: data can be reused and analysed to provide support for marketing or managers' decision-making (see for example Flyverbom, 2019; Gillespie, 2014; Lupton, 2016; Zuboff, 2019). The production and use of digital traces for digital data recycling are also an important part of thinking about new ways of working that aim to operationalize knowledge-based policing through sharing and managing collected data, which is supposedly a more politically neutral and objective form of knowledge (Chan et al., 2022). Awareness of the value of digital traces enables new strategies for knowledge production, while old-style knowledge production is modified by access to new software for data integration.

One objective of the intelligence process is to make uncertain knowledge less uncertain by applying social science methods to «ensure the greatest possible degree of objectivity and validity» (National Police Directorate, 2020, p. 37). However, within intelligence studies, the view that intelligence is objective and politically neutral has been questioned (Fyfe et al., 2018; Rønn, 2022). According to Rønn (2022) intelligence studies has defined objectivity in a variety of ways: as the positivistic ideal of interpretation-free objectivity, as value-free objectivity, (value-neutrality), as detachment, and as fairness. Most interesting for our study is the Intelligence Doctrine's view that objectivity will distinguish between data and personal values:

It is important to distinguish between information obtained and the analyst's own assessments. The analyst's assessments are influenced by many factors, such as background, experience and professional qualifications. To overcome this and ensure the greatest possible degree of objectivity and validity, social science methods must be used, (National Police Directorate, 2020, p. 37).

The doctrine thus views data as raw, and discussions of this will be at the core of this article. The doctrine does not lay down which social science methods should be used, but the main principle

is that data is raw, and that the highest degree of objectivity is achieved by minimizing personal values and experiences (Rønn, 2022, p. 824). This is very close to what Rønn terms the scientification of intelligence, «in which science and intelligence are understood as two sides of the same coin, and the norms of intelligence are considered equivalent to the norms of (positivistic) science» (Rønn, 2022, p. 830). This scientification of intelligence is why we use the third term 'epistemic power' when analysing the results of datafication in police officers' everyday lives. According to Archer et al. (2020, p. 29) epistemic power can be defined as someone's power to influence what comes to be regarded as knowledge: «A person has epistemic power to the extent she is able to influence what people think, believe, and know, and to the extent she is able to enable and disable others from exerting epistemic influence.» As we said in the introduction, we define epistemic power as the power of definitions, narratives and items on an agenda that does not necessarily require legitimate sources. Epistemic power might therefore be seen in what are perceived as reliable and credible representations of knowledge, whether they are based on legitimate sources or not. Since epistemic power is an outcome of socio-cultural categorizations, we are also inspired by the cultural theory of Mary Douglas (2002) in our analysis of user experiences. As Bowker and Star (1999) point out, Douglas's cultural theory of categorizations is an early attempt to understand the social construction of classification systems, and how it is related to symbolic and cultural values. Exploring the use of digital traces

in the practical, symbolic and learning dimensions makes it possible to understand this use from several angles. Domestication theory's roots in both STS and media studies underline the importance of bringing together cultural and material dimensions to understand why digital traces are used in different ways by different user groups.

There has long been discussion about the politics of knowledge production, with debates about the relationship of power and knowledge being most prominent in post-structural Foucauldian theory, which has decisively shown that, since power relations are always bound up with knowledge, knowledge can never be said to be disinterested or neutral (Foucault, 1977). Science and technology studies (STS) have considered how processes of classification and standardization shape politics, both «arriving at categories and standards, and, along the way, deciding what will be visible or invisible within the system», (Bowker & Star, 1999, p. 44). Bowker and Star argue that, since they are powerful technologies, «classifications should be recognized as the significant site of political and ethical work that they are.» (Bowker & Star, 1999, p. 319). We will engage with this idea by discussing different perceptions of the epistemic power of recorded data and digital traces, and how they relate to the particular professional and contextual environment a practitioner belongs to. We therefore examine processes of sense-making, practice and learning related to recorded police data and how this produce, or does not produce, epistemic power and aim to name these.

## Digital tools and concepts in Norwegian intelligence-led policing

Intelligence-led policing has a long history (Ellefsen & Lomell, 2024). The above-mentioned Intelligence Doctrine represents a new stage where intelligence is not only implemented as a process, but as an overarching management concept with new police roles. Moreover, the doctrine was central to the recent police reform, where intelligence was one of the six functions that was relied on to make the police more proactive and risk aware (Gundhus et al., 2022). Intelligence-led policing aims to be a controlled process consisting of the systematic collection, analysis and assessment of information about individuals, groups, and phenomena, to form the basis for decision-making (National Police Directorate, 2014, p. 18). The doctrine lays down principles and standards for a decision-making procedure known as the intelligence cycle (National Police Directorate, 2014, p. 13); it is the traditional approach of various agencies to conceptualizing the intelligence process (Phythian, 2012). Its five steps are planning, collection, processing, analysis, and dissemination; the latter is highly dependent on the processing of data. The cycle begins by identifying management's 'information needs', and acquiring relevant data from databases, reports or human sources. The collected information is then processed, analysed, and assessed, and the resultant intelligence products are disseminated to managers for decision-making on interventions, operations or prioritization (Vestby, 2018).

Indicia, the Norwegian police's crime intelligence register, is the main digital tool used. It was developed specifically for the police and was launched in 2006. Indicia is regarded as the main search engine for intelligence practice, searching in all the main police registries. This is regulated by the police register regulations (Politiregisterforskriften, 2013). The police can record a wide range of information, such as details about offenders and their affiliations, and about individuals who are believed to be likely to engage in criminal activity. IBM's i2 Analyst Notebook, is also used, for both operational and strategic purposes, to visualize data patterns from different police registers. Analyst Notebook has been used by Norwegian police analysts since the late 1990s to visualize networks within organized crime and terrorist networks in both investigation and intelligence.

A central aim is to make further use of intelligence products within the police organization or to share them with collaborative agencies, such as customs and municipalities. This is briefly described in the doctrine as the intervention process governed by the manager (National Police Directorate, 2020, p. 52-53). A handbook has been produced to support the implementation of the interventions, known as KUBA, (knowledge-based policing), (Norwegian Police, 2020). The cases we will analyse in the article both involve making decisions in police districts on the basis of intelligence reports.

One is a geographical unit in Central Police District, where a crime prevention unit ordered an intelligence report. The other is a geographical unit in South Police District, which was conducting a broader KUBA intervention. In a KUBA intervention a crime prevention unit coordinates an intervention group comprising managers from crime prevention units, investigators, patrols and the chief of police to prioritize resources and measures. After intervention meetings, the managers and those responsible for each measure are tasked with ensuring implementation of the measures and prioritization in the assignment process. This might involve sending police cars to areas at risk. The police control room then oversees interaction and prioritization in the planned measures and the incidents that are occurring. Patrol managers also have an important role in gathering enough data to make intelligence reports.

In intelligence theory, a central idea is that intelligence should contribute to a shared understanding of the situation and be a common starting point for choosing interventions across disciplines and levels in the police (Ratcliffe, 2016). Intelligence should also be used in operations or more strategic plans to assess future threats and be shared with relevant societal actors, to help individuals and society prevent crime and undesirable incidents by protecting themselves and their assets (National Police Directorate, 2020).

Intelligence reports are therefore made to facilitate interventions. In intelligence theory this is formulated as a requirement for intelligence to be actionable: it should provide the background information that is necessary for dealing efficiently with a specific situation, in the short or long term.

In addition to assigning this function to intelligence, the police reform also involved a reorganization, which reduced the number of police districts from 27 to 12 (Prop. 61 LS 2014-2015). The police were organized in two levels, with the chief of police in level one and the functional and operational units in level two. The operational units were divided into several geographical operational units at the same level as the functional level. Functional units provide support for all the geographic units. Most of the police's work is carried out in the geographical operating units, and the functional operating units are organized to support them. The functional units assist with intelligence, investigation, prevention, prosecution, immigration, administration and civilian tasks, in addition to being the main seat for the police control rooms (National Police Directorate, 2017). How the support functions are merged into joint units depends to some extent on the size and needs of the police districts (National Police Directorate, 2017). In this article, the functional intelligence unit is seen as being of special importance to the geographical police units' work on intelligence analysis.

## Methodology

The empirical material is taken from two related research projects: Critical Perspectives on Predictive Policing (CUPP) and Algorithmic Governance of Policing (AGOPOL). The research projects are related, since both explore cases where digital technologies are used in intelligence-led policing in Norway.<sup>1</sup>

AGOPOL examined cases in three Norwegian police districts, anonymized as West, North and South, and an IT project in a special unit. Our selected case- Case A- featured the most in-depth investigation of an intelligence-led policing project, a project carried out in a geographical unit in South district. We looked at how digital traces are used to decide resource allocation and prevent both present and future crime. The process follows the Intelligence Doctrine, first the making of the intelligence report, and secondly what we previously presented as KUBA intervention, to make interventions based on the intelligence report (The Norwegian Police, 2020). Twenty-one police officers in various positions were interviewed: managers, investigators, patrol officers, and intelligence staff. Police patrols were observed for a total of 50 hours. This case can be seen as a 'prototype' of the use of digital traces and other forms intelligence, and provides important insights into practices that have developed over time. The A-case interviews were conducted jointly by Gundhus and Wathne.

The CUPP research project consisted of only one case in a geographical unit in Central Police District, which we will here call case C. In it, intelligence was used to identify and target, within their geographical area, 'young people at risk', who might be on the threshold of becoming criminals, so that early intervention measures could be taken. This was carried out at a police station. A traditional crime prevention unit (CP unit) collaborated with an intelligence unit to prevent youth crime which, for Norway, was an unusual and somewhat controversial initiative (Gundhus, Skjevrak & Wathne, 2023). It was a new approach, where intelligence analysts in a local police station tried to identify 'candidates' for early intervention through data in police databases (for a fuller description, see Skjevrak & Gundhus, 2025). In relation to it, approximately 17 hours of observation were carried out, and 18 people were interviewed in 14 interviews. Seven of the interviews were with key informant crime prevention police officers (CP officers) who took part in C. We also conducted interviews with five crime prevention specialists in the police district involved, two legal professionals, and a group of five officials from the National Police Directorate, which provided contextual information on crime prevention strategies and youth crime prevention in general. Most of the C interviews were conducted by Skjevrak, some were done by Gundhus.

<sup>1</sup> Gundhus participated in both projects, Skjevrak was involved in CUPP, and Wathne in AGOPOL.

Gundhus and Wathne also interviewed fifteen ICT-related employees from the National Criminal Investigation Service (Kripes), Central Police District (CPD), the National Police Directorate (POD), the Police IT centre (PIT), and the Police University College (PHS). The choice of such a broad range of informants was designed to shed light on the variety of practices followed, and to understand the logic behind them. Our aim was to identify different perspectives, experiences, and unwritten practices, though in this article, the interviews mainly provide context for the domestication practices that we identified.

In addition to interviews and observations, in both cases we also draw on documents such as plans, minutes of meetings, and internal evaluations. These documents provided important background information about the intelligence projects' goals and their results, information on such things as how digital technologies were supposed to contribute to the intelligence process, and how they were perceived as solutions to the challenges in question, and what was thought about their results.

The interviews were semi-directive, so that informants could talk spontaneously and cover as many points as they wished, rather than being constrained by the order of the interview questions. We used thematic analysis for the initial coding and analysis of interviews, inspired by Braun and Clarke (2006). Codes and themes across the material were identified inductively, supported by a subsequent abductive process addressing theory. We also made use of situational analysis (Clarke et al., 2018). This is an extension of grounded theory, which helps address the shortcomings of a strictly inductive approach (Clarke, 2005, pp. 11–16). It is inspired

by Foucauldian discourse analysis and social studies of science and technology, and was therefore appropriate for this study, where the focus is on analysing elements of situations and relations between those elements, the conditions for possible action, and related discourses—to ensure that differences became more visible. The individual interviewee's perception of situations is related to the wider network and subgroup they belong to, because we are particularly interested in similarities and differences in the practice of managers, CP officers, intelligence officers and front-line officers. All quotes and documents were translated from Norwegian into English by the authors.

The projects received the National Police Directorate's approval to observe the police. Interviews and observation were conducted following approval by the Norwegian Agency for Shared Services in Education and Research (SIKT), which is responsible for enforcing ethical guidelines, and following authorization by the chiefs of the police districts and the National Police Directorate. Each participant, recruited on a voluntary basis, received, and signed, an information sheet about the project, which outlined the aims, methods and implications of the research, the process of anonymization, ethical guidelines, and data management, as well as their right to withdraw from the project at any point.

To distinguish the two projects, quotes from A project interviews are marked 'A' and those from C are marked 'C'. The position of each interviewee is indicated. Intelligence analysts are marked 'IA', crime prevention officers 'CP', managers 'M', patrol officers 'PO', and IT personnel 'IT'.

## Datafication workflows

To understand which factors that shape how digital traces are used, we will now present in more detail the practices the technologies are part of and the context of the police officers' negotiations with these technologies. The intelligence cycle is described as a process that is designed to organize how the police acts and governs itself. It assumes that the recording of data and its visibility facilitates knowledge sharing and learning from experience. Since data is fundamental to the intelligence process, the selection, quality, and compilation of the data recorded is of great importance. New police officers are taught that sharing data for decision-making is the correct way to produce knowledge. Intelligence-led policing aims to change routines and practices and, as we will see, available digital traces represent a very specific view of the knowledge, which determines subsequent interventions. These are highly dependent on the digital traces in police databases, but these traces are seldom used in a linear way (Lundgaard & Gundhus, 2024).

Features of the Indicia crime intelligence system follow the intelligence cycle that was later set out in the Intelligence Doctrine, as one informant described:

Indicia functionality follows the Intelligence Doctrine process to the letter. We have prioritized functionalities for 'intelligence needs' from which police officers derive hypotheses. We therefore link 'information needs' to hypotheses and ask for specific data to be gathered. The resultant information can then be linked to 'information needs' and hypotheses. That way the entire intelligence cycle is covered. (IT personnel, A)

The doctrine suggests that data gathering is directed by hypothesis. As we will see, in practice, (and this is confirmed by a data controller at Kripes), the data put on the system is generally not a hypothesis to be investigated but simply information related to persons, phenomena or events. While all police officers had access to the system, the extent of their access varied. An intelligence analyst specializing in organized crime usually had more extensive access than a patrol or crime prevention officer. The increasing importance of what is stored in Indicia was described by an intelligence analyst:

*So, for handling the information that is important for knowledge-based policing and preventive measures, Indicia is the only database that*

*works. Because things are different now from ten years ago, as far as the use of recorded data is concerned... Society as a whole has become much more complex as regards the amount of information there is, both in criminal cases and everywhere else. Telephones, data traffic, social media... You have a completely different network now from what you had before. So, Indicia is much better than the other systems in terms of being able to handle, sort and systematize large amounts of information. (IA 1, A, 2021)*

In this quote, the analyst expressed the epistemic power of Indicia. If information is more smoothly handled, it made knowledge appear more valid. Indicia was perceived as a good solution for searching and systematizing data from the different police databases, even though the search engine did not integrate the data: officers must log in and out of the police registers to get more information about the result of a search. There are dozens of systems and registers, and in the interviews a perception often expressed was that the basic police systems were old and unable to «talk to each other». Although Indicia is well thought of as the main search engine for intelligence practice, other software, such as the i2 Analyst's Notebook, described above, was used for visualizing, interpreting, and analysing data. Due to privacy regulations, when data was selected for further analysis, it was not transferred directly to Analyst's Notebook from police systems but first imported into

Excel to be structured and categorized. These procedures are very time-consuming and manual, as was made clear by interviewees. The process of checking data and making it ready for analysis in Analyst's notebook was based on discretionary assessments. The extraction, structuring and processing of data—what is called the cleaning process—was therefore not fully automated and demands manual work.

Division of labour between the collector of the information, the analyst and the commissioner of the intelligence assignment led to a divide between data collection, analysis, and decision-making. The aim is greater objectivity and a reduction of subjective discretion. Patrol officers must document what they do in the police register, and this should be immediately visible in Indicia and on their mobile phones. This is a step towards datafying the police, with work processes moving to digital systems and communication and collaboration taking place via distributed digital arrangements. The Intelligence Doctrine requires all information used to be recorded in Indicia. The police registers therefore act as 'digital prisms' that refract, categorize and organize data into distinct configurations and novel forms of knowledge: «digital technologies afford particular ways of managing visibilities, and shape what we come to see, know and govern – and not see, know and govern» (Flyverbom, 2024, p. 3).

## Practices and sensemaking—the making and managing of digital traces

In this section we will explore various police officers' experiences of carrying out intelligence-led policing: as regards their practices when entering data, interpreting data and making subsequent interventions.

### Practices

Although the interviewees perceived Indicia as much better than other systems for managing, sorting and systematizing large amounts of information, there was general agreement that what was recorded is random and coincidental. The arbitrary recording of data is therefore a key aspect of the domestication of digital data recycling. That being so, several information handlers described the data recorded as biased. For instance, one patrol officer said:

*I know what I write in Indicia now will form the basis for the next KUBA [knowledge-based policing] period because it changes three or four times a year. And then it is... I think we've developed a lot, but we can get better at writing and sharing information in those systems. You can see that only a few officers, perhaps 20 %-30 % of us, write 90 % of it. (...) A small percentage write most of the messages in the intelligence system, and why is that? (PO, A, 2021)*

The officer argued that data visible in the police database is biased, since it is shaped by police officers' interests and motivation. For the police officers on patrol, it was obvious that the data recorded is selective. Several beat officers were clear that data is not objective in terms of raw data, since a lot of possible data is

absent; they agree in thinking that data is biased, selective and partial. Moreover, in their view, uncontextualized data which lacks relevance and richness, for example details on people and the relations between them, or geographical information about places, was of little use to police officers patrolling the streets. The lack of context accompanying the information in the police databases was discussed at length during our observations of patrols in case A. In their experience, data retrieved from the police data bases lacked substance, and their criticism of data quality echoed what Flyverbom describes as follows:

In processes of refraction and reconfiguration, contextual and many other features may be lost, and if we make inferences based on data alone, they may be based on selective, biased or partial information. This is so because when humans or social phenomena are reduced to data points and sorted out algorithmically, their origins and richness may be lost or made invisible. (Flyverbom 2024, p. 4)

Although the analysis staff responsible for the intelligence report can ask officers to gather specific information to meet so called «information needs», there are huge differences in whether, and how this information was approached, gathered and recorded by patrol officers. In the interviewee quote above, we also see that while everything that counts as relevant information and knowledge was supposed to be registered and available, few patrol

officers followed up on this. The data put into the system was highly visible, but few officers were sufficiently motivated to record all the data that was supposed to be there. One reason was that this data was gathered for the central functional unit, and not for local purposes. Here a local analyst lamented the failure to ask local units for data:

*But the central analysis unit are dependent on local knowledge. If they need information for a case, they do some searching in the systems themselves. They could identify their information needs and ask for it, which we might be able to help with. But this probably won't be done, due to resources and their faith in the intelligence that has already been recorded... But this [identifying information needs] should probably be done much more than it is at present. (IA 1, A, 2021)*

Patrol officers also criticized intelligence reports for lacking local contextual knowledge, which meant they had to search the police registers for useful information themselves. To make good analyses, the central unit was dependent on local knowledge, just as the local police was dependent on information from the central analysts. However, what was recorded in the police registers was not just data that someone wanted to register, it was also data that was accessible and could be registered and stored. This was what came up as valid data, despite not having been verified or quality controlled. For patrol officers, the richness of contextual data was important, and was lost when their own observations and experiences were reduced into digital data. These perceived shortcomings in the data affected how it was used and therefore the domestication of digital data recycling. The police officers' views thus chimed with Flyverbom's notion that «what we encounter as data is not the same as the phenomenon that was turned into data points» (Flyverbom 2024, p. 4).

### Sense-making

Several interviewees said that the data recorded in police registers is guided by intuition, not the information needs set out by the analysts. Analysts, for example, felt that what was registered was random and often determined by gut feeling:

*You don't have a very conscious idea of what kind of information you're trying to get hold of. You kind of get... You get a bit of random information like that, and then you write it down, and then you see if it fits. It's like you're not trying to get what's being asked for. And it's actually a bit strange, because the police are good at police operations, you're good at targeted investigation, you're good at a lot, but... It's just that when it comes to the information that... It's called intelligence information, which in a way does not seem connected to a criminal case or other things that may be important, we are probably not clever enough to be goal oriented. (IA 1, A)*

In the quote above, the intelligence analyst touched on the logic of selectivity when he said that the police enter random information. What was entered in Indicia, he said, was a matter of whim and personal interests, rather than being information asked for by

analysts to make assessments. Perceptions of what information was important was based on intuition, emotion and feeling, in a way comparable to the epistemic power of experience and gut feeling within police occupational culture (Cockcroft, 2020; Gundhus, 2013). This emphasis on gut feeling chimed with Brayne, Rosenblat and Boyde's observation that much of the information police officers put into the system was there because of their intuition that this data was important, rather than because they were trying to meet more official «information needs» flagged up by the manager (Brayne et al., 2015). In the quote below, we also see how an intelligence analyst chose to rely on gut feeling, despite knowing that objectivity was what was required:

*One of the basic principles of the Intelligence Doctrine is the requirement for objectivity and integrity in the work we do, and we strive to be objective at all times. Gut feeling isn't objective, it's subjective, isn't it? So, I relate to data. And I can have a gut feeling, and maybe often it is right.. Or it is right. I think- 'I should look at this guy. Ah, it was a good thing I looked at him, because he was relevant.' (IA 1, C, 2021)*

As the intelligence analyst argued in the quote above, despite objectivity being the rule, data was shaped by construction: it was interpreted and made sense of. Following Douglas' (2002) cultural theory, the intelligence analysts' reflection can be viewed as representing a break with ordered relations, which threatens the boundaries of the cultural system. By defining gut feeling as a possible source of important knowledge, the boundaries of the epistemic power of recorded data are challenged. The same intelligence analyst went on to reflect on the process where young people was selected as suitable candidates for early preventive measures through discussions with the crime prevention officers:

*It may not be so emotion-based, but in the selection process, we (intelligence analysts) select the young people we think are suitable. (...) And sometimes we hear back [from the crime prevention officers]: 'No, these ten people were not suitable.' Then I might think: 'But it was strange that they weren't suitable.' I don't necessarily get to know why they are not suitable. But it is perhaps this type of situation which is the only time I can think of when there could be surprises. Or conflicting thoughts. (IA 1, C, 2021)*

Why the interpretation of data also affected digital data recycling can be understood as a background element in the interviewee's story above. We see in it a distinction being made between a 'pure' digital system characterized by objectivity and rational thought on the one hand, and a 'dirty' human approach characterized by gut feeling, subjectivity and emotion on the other. This accords with the distinction made in the Police Intelligence Doctrine, which speaks of new data-driven methods and intelligence products helping to create a more objective and scientific basis for decision-making (National Police Directorate, 2014). The aim is to 'domesticate' subjective information possessed by individual police officers, by turning it into data and making it part of the intelligence cycle,

in which analysts should be objective and not make suggestions. When the intelligence analyst in the quote above reflected on the crime prevention officers' decisions on who should be kept on the candidate list, he showed that «he relates to data» and relied on it. Intelligence officers provided analyses of quality-assured data. This quality assurance was talked about as a cleaning process, during which they distinguished between clean and dirty data, even though they were aware that the objectivity of the data was questionable. For them the 'impure' was what flowed across boundaries and messed up the 'clean' stuff (Douglas, 2002).

The use of tools and processes which turned their work into quantifiable data that could be tracked, monitored, and analysed, and the requirement to discard experience-based knowledge, caused police officers to lose motivation, and forced them to navigate the process of datafication. One example of this appeared in the way experienced crime prevention officers in case C felt that they lost their value and professional pride when the task of selecting candidates was transferred to the intelligence analyst:

(...) I was told that many of the old crime prevention officers felt that they had no value anymore, as it was the intelligence unit that was supposed to produce it [the knowledge] - I told them 'It's a new age.' I remember I taught on an intelligence course that some of the older people were on. I said that you must now register on Indicia the information you get. If you enter it into Indicia, then intelligence will pick it up, and that information will be included in the next report. And that's how you make your work visible. But they didn't want to (CP1, C, 2023).

The quote above makes clear gains and losses resulting from putting data into the system. The obligation to file information is rewarded with recognition for the police officer's work, and its appearance in the next report. But this reward had no motivating effect on «old school» crime prevention officers, who became either non-users or reluctant users of the technology. It made them think that they were now worthless, and that intelligence would produce knowledge for them:

(...) some people believed that working for 15 years in the preventive field, in the same area, and with all the experience you get, made them better able to make judgements about

whether someone was in trouble than these cold computers in the analysis office. (...) those who had been working for a long time were very negative about [name of the crime prevention project]. They thought it was difficult, and a pain and they were not used to registering their information. After all, these were people who kept things in binders, or in their own computer folders (CP1, C, 2023).

The older generation of crime prevention officers were reluctant to comply with the new requirement to put information about young people on the system. In interviews, they told us that delegating this task to the intelligence analysts also deprived them of one of the crime prevention officer's key tasks. The project targeting young people at risk required the crime prevention officers in the local unit to digitally record information that previously had often been kept in personal folders. This led to dissatisfaction among officers because of the increasing demand for documentation, which was time-consuming and meant that more time was spent «inside» in front of computers. This lack of motivation, which led to reluctance and even resistance, reduced the use of digital traces and can be understood as a dis-domestication of digital data recycling (Ask & Søraa, 2024, p. 76-77). The use of digital traces did not fit into the crime preventers' professional ethos or their everyday lives. This new data-driven approach marked a shift in their role, whereby transparency and accountability were paramount, in contrast to previous practices, and aligning more with the analytical approach of the intelligence unit and the younger generation of crime prevention officers (Skjervak & Gundhus, 2025).

A key point made in this section is that meanings ascribed to the processes of data-driven approaches and the sense-making that took place reflected a division of tasks and decision-making. Police officers patrolling the streets or meeting young people face-to-face felt less obligated to the recorded data and intelligence reports. This raises questions as to whether intelligence-led policing contributed to knowledge sharing or knowledge separation. We argue that, while the goal was to share more knowledge, the division of labour between the intelligence analyst and the crime prevention officer also led to a devaluation of experiential knowledge. However, data that was stored was valued and regarded as significant for making interventions, which is something we will turn to next.

## Learning – «if something does not exist in writing, then it does not exist at all»

All use of technologies requires some kind of knowledge and skill, be it operational skills or knowledge about their appropriate use. The last dimension we will explore is how learning and knowledge shape the use of digital traces.

We have pointed out that in the KUBA project, the central analysis unit rarely asked local units for data, while the patrols found that the unit's analyses lacked local knowledge. They had to search police records for useful information themselves. However, to make good analyses, the central unit was dependent on local knowledge, just

as the local police needed information from the central analysts. If the selection of data depends on hierarchical sharing of data, it is difficult for local intelligence officers to know what is going on. Central and local police may thus have different knowledge bases, which can lead them to give very different answers to questions such as «what is the most important challenge?» In intelligence, this question is a central tool for prioritization. We argue that, because the data flow is functional, systemic, and limited, there was little opportunity to criticize the data. It was not questioned or scrutinized in a learning forum (Gundhus & Wathne, 2024).

The knowledge recorded was to a certain degree delegated authority that was open to negotiation. Our analysis implies that it was difficult to negotiate data when it was embedded in the ICT systems. Data was either stored or not stored, and there was no scope for questioning what had been recorded and what had not. One option was simply to reject, ignore, or resist the doctrine by not registering on the system or using information in the system in an alternative, unintended way (Gundhus & Wathne, 2024). However, digital traces were inevitably domesticated in the subsequent process of creating an intelligence report. The basic discursive assumption of the doctrine was that aggregated information should be perceived as superior to contextual knowledge, and this was a challenge for police patrols. Contextual information lied *outside* the police database and therefore often resisted datafication:

Yes, there is always someone working in the police who knows something about that person or the area around there, who lives there or something. I don't think they [analysts] are good at connecting with people [police officers] who have plenty of local knowledge. The big machine [intelligence cycle] just keeps on going. (...) But again, if you follow the rulebook, which is one way to solve the problem, then you're in the clear, as I understand it. (M PO, A, 2021)

Only information that was recorded in the system was used by intelligence analysts, to make valid information for the intelligence reports given to the police district managers. Digital traces were a key component of what analysts later used to make reports. This meant that, for them, only data stored in the system was actionable knowledge – and it was from this that conclusions were drawn, as this intelligence manager described:

We try to be aware of the need to be objective. We are human, so there is always a danger that bias will come into play. But if something does not exist in writing, then it just does not exist. And it may well be that our assessment is wrong, and that [an officer in the village] knows that a person is not dangerous, but that has not been written down anywhere. If it hasn't been made available, we are not allowed to use it as a basis for further assessments. So, it is difficult for us to say anything about it. And that's why I say that, in a way, writing is absolutely necessary. And that is why we bear in mind the value of what is produced. So that we can produce more of the right kind of thing. If our

premises are correct, the assessments will also be more correct overall. (IA 1, A, 2021).

According to the Intelligence Doctrine, only visible and recorded data was valid, and it was this data that contributed to subsequent knowledge production. Data which was not on the system did not exist. What counted as valid data, also depended on the system's user interface, design, and layout. Some changes have been made to attract police officers' attention, for example regarding the type of information they should collect when they are on patrol:

A lot can be done to make it [the interface] nicer and better and maybe a little more intuitive, but it's much better now than when you just got a list of lots of events. Because that's what the police did back in the day, when they went in and got a list of events and there'd be something about drugs and like, 'that tip there on drugs, we can just go to this area,' (IA 2, C, 2022).

As the interviewee said, a more user-friendly design could also motivate patrol officers to be more aware of intelligence analysts' need for information to improve the quality of reports. Sharing intelligence reports can potentially also increase officers' understanding of the importance of this work and encourage them to help make knowledge digital and valid. Elsewhere in the interview, this informant emphasized that what we term the epistemic power of recorded data varies, depending on the user interface. Although data was based on insecure and biased inputs, what was recorded had authority, since it must be negotiated, corrected, used, or not used, and since digital traces had to be acted upon in one way or another. In a previous study, we described crime prevention officers' use of the Signal app—secure and private messaging app—that police officers downloaded to their phone to share pictures of young people and information about them (Gundhus, Skjervak & Wathne, 2023). This use had now been stopped by police managers, showing how external factors (such as legal regulations) also affect (and can be setbacks to) domesticated communication practices (Hartmann & Hartmann, 2023). One of the informants said this led to more time-consuming practices requiring officers to go into systems only accessible from the car:

It's not just inappropriate, it's not legal. So, what we do now is go into the media link in the case and look at pictures. So, then you have to get into the car. And so, it becomes less efficient. (WG 5, C, 2023)

In other instances, however, doing computer work in the car was described by this informant in more positive terms, since it was better than driving to the police station. As already mentioned, CP officers expressed dissatisfaction with all changes that meant spending more time in front of computers, either inside the car or at the station, since it took time away from being outside, where what they deemed to be the real preventive work took place. This attitude is not unique to the intelligence project targeting young people. Our interviews with officers from various police districts in Norway, involved in the AGOPOL research project, found

general dissatisfaction with the increased obligation to document observation and gather data in the police registers. There was impatience with writing and documenting everything, whether the officer had to do it in the car or at the station. In the A-case project, officers on patrol found writing in their cars difficult. There were issues with smaller hardware formats, and it was difficult to hide them from people passing by. Another informant said a new phone app made it a lot easier to register on the spot, describing it as a «speedway to recording things» (WG4, C, 2023). Thinking about what should be recorded and what shouldn't, he said:

I don't have a good answer. I'm very curious about it myself. It becomes very subjective. I walk through a shopping centre, and just at that moment it happens that this place is quiet. Or the opposite. Because I get involved in a youth conflict there, it can quickly become 'true' that every time I am in a shopping centre there's trouble with young people. There is the danger that there will be some random examples from which you make a big picture a little too quickly. (...) If you write a report at the end of the evening, there is a greater chance that you will only include the negative. The advantages are probably that you get a lot more information, and hopefully also more positive information. The disadvantage may be that what an officer experiences once in a while can quickly become a general truth. (WG 4, C, 2023).

Several interviewees talked about the pros and cons of registering data while on patrol. For example, one of them argued that user interface was important for smooth processes.

In this section, we pointed out that only information that was visible on the systems was acted upon. Everything that counted as knowledge must be recorded. Those who advocated using technology to document police practices and make them more accountable argued that documentation could reduce problematic biases in police practices related to race, class and neighbourhood. Documentation would then function as an accountability mechanism, since the decision maker must justify discretionary judgments (Molander, 2016). Documentation is something that should be done for the sake of others. Instead of relying on officer intuition, intelligence-led policing, in theory, relies on data, which can standardize information across work periods and levels of experience, eliminating concerns about adequate information sharing. However, as argued by Brayne et al. (2015), it is important to avoid false binaries such as 'intuition-driven' versus 'data-driven' policing, because in practice, neither approach exists in isolation: each informs the other in consequential ways. Since the interviewees in our cases did not talk about data as either intuitively generated or data-driven, this is also confirmed by the empirical findings in the two cases. Contextual aspects related to the user interface, for example, affected what was intuitively seen and recorded in the crime intelligence database.

## Discussion

According to the Intelligence Doctrine, only visible and recorded data is valid and contributed to subsequent knowledge production. Data that was not in the system did not exist. In this article we have highlighted user experience and perceptions of data's epistemic power. However, what counted as valid data was also affected by the system's user interface, design and layout. We have therefore shown that what we term the epistemic power of recorded data varied, depending on the user interface. Despite data being based on insecure and biased inputs, what was recorded acquired authority through being negotiated, corrected, used or not used, because digital traces must be acted upon in one way or another.

We therefore argue that police employees' different professional roles and positions in the police organization shaped what technology meant to them and how they used it. Interviews with police officers in different roles indicated that the epistemic power of digital traces varied, according to contextual factors such as whether they were crime prevention or patrol officers, and what crime challenges motivated them. However, since only recorded data was valid in knowledge production, it was difficult to negotiate and challenge the routines connected with the making of this knowledge.

Both our cases showed that the domestication and digital recycling of data in the police organization was shaped by the users' everyday life, rather than by a passive use of technical devices (Jasanoff, 2004).

Moreover, when data was collected, a choice must be made from the limited amount of data that can be or has been collected, and that was retrospective. The selection of some data rather than other data entailed a tacit retrospective creation of meaning. The data collected had potential meaning and acquired importance by virtue of the fact that it had been collected. In contrast to other observations of social phenomena, this data was transformed and recontextualized as something else and something new: what Flyverbom (2024) refers to as «refraction». However, this data could have been understood, interpreted, and classified differently, had it been categorized differently or refracted through other data. This is significant for classification (such as sorting or «cleaning») and for selection (such as prioritizing what to act upon). It is difficult to question data that has been recontextualized. Once the data is coded, the context is broken down into bits that can be approached and used as data points (Flyverbom, 2024). Once it is categorized, recontextualized, and written into a report or an intelligence product, its contextual richness will have been lost. The data recorded in Indicia was very much value-based, but appeared detached from the morals, norms, values, connections, emotions, contexts, and situations surrounding it when it was recorded. Although the data was classified as being of varying reliability, it acquired the status of validity by being made into something neutral and objective that could be measured, indexed, read, and searched. In reality, there was a lot of data that could not be retrieved because it was not registered.

This gives recorded data a certain epistemic power regardless of how users domesticate digital traces. We argue that information that was seen and acknowledged to be uncertain conferred authority to be governed and steered by the users. However, it was not the uncertainty that gave this authority, but the data's visibility in the system, which meant it must be interpreted and managed by its key users, most often the intelligence analysts. The intelligence process was constrained by bias inherent to the system, which resulted from focusing information gathering on what was already available, and from connecting it to recurrent individuals and problems. Intelligence cycle data was bound to be based on «searching across existing data to locate new and emerging risks» (Innes, 2006, p. 230). The knowledge produced and which guides decisions was therefore

(...) not neutral, objective representations of a reality out there, but rather (or at best) proxies (Mulvin, 2021) or digital doubles (Haggerty & Ericson, 2000) that often come to stand in for the individual or the social phenomenon under scrutiny. This obviously raises important questions about the accuracy of and correspondence between the

proxies and the actual phenomena. (Flyverbom, 2024, p. 4)

This brings us to the implications arising from this. We suggest that datafication can be understood as a central domestication practice where the introduction of digital tools into police patrols and to crime prevention officers separates knowledge management processes into different functions in the organization and thereby reorganizes everyday police routines. Depending on whether the data is perceived as proxies or the true situation, there is variation in how it is interpreted and in subsequent learning from it, depending on the officer's proximity to or distance from the reality that the data represents. The difference in cultures between police at street level and managers, famously referred to by Reuss-Ianni (1993) as the divide between street cop culture and management cop culture, can also be understood as a factor in the variation. When digital tools are domesticated in policing practice, it can become part of police officers' understanding of themselves and of their broader social relations to the public. It may then lead to a divide between a 'datafied-cop culture' and a 'contextual-cop culture'.

## Concluding remarks

Our main finding is that digital traces were not necessarily used as the steered and managed intelligence process envisioned in the Intelligence Doctrine, and that this led to various adverse outcomes. However, we argue that digital traces were of great importance, even if the data was uncertain, because of the status they acquired in the intelligence process. The data provided some instructions for use which did not need to be followed, but the police must relate to them in some way—either rejecting, resisting, ignoring, supporting, adopting, or negotiating them. Police officers therefore related to, made, and used digital traces in various ways, including ignoring them. We have also showed that the intelligence process required digitization, which involved simple processes of turning analogue objects into digital ones, by converting police observations of the environment and information from reports into digital formats. In this process police officers' gut feeling and intuition still mattered, for example when information was selected for the crime intelligence system.

In both the cases discussed, the Intelligence Doctrine was important in providing guidelines for how data processing should be managed. However, despite agreement on how data should be applied, differences in practical routines, the digital tools used, symbolic work and learning processes revealed that its domestication in the police organization was messy: everyday life and technology was both re-shaped, rather than it just being a matter of technical devices being adopted. We found gaps between policy and practice, which can be seen both in unexpected workarounds and in solutions for organizing routines and everyday work. Hands-on tasks in policing, including the use of tools and the handling of data quality and reliability issues took on various patterns in routine practice. These reciprocal processes both influenced police occupational

cultures and were themselves influenced by them. For a deeper understanding of these two-way processes, we need more research.

The epistemic power of recorded data had the potential to undermine the meaning of local knowledge and devalue those who possessed it. We suggest that the Intelligence Doctrine therefore constitutes a symbolic structure in which ambiguous police work processes are codified and institutionalized (Douglas, 2002). The local context did not fit the structure of the new digitized work process: it was a stream that flowed across organizational borders. The domestication of digital data recycling thus conferred new epistemic power by making certain things visible and clean, while leaving out facts which were difficult to categorize and showed up as 'dirt'. The way the police related to the epistemic power of the data varied, but officers were obliged to relate to this uncertain element. How the digital traces were made, used and interpreted also depended on training and education. Intelligence is a developing discipline within the police, and the way recorded data is interpreted and utilized, might therefore change in future police projects. It will therefore be of interest to continue researching what happens when technologies are (tamed) and brought into the police domain, particularly when more hidden algorithms and artificial intelligence applications have been adopted. To what degree will police officers have to choose between supporting the narrative created by stored data or the narrative created by other observations? Here, the social identity of the police might come into play, since work practices characterized by datafication might also affect self-identities associated with either a 'datafied cop-culture' or a 'contextual cop-culture'. Future research will show whether these contrasting binaries can be better described as a continuum.

## Acknowledgements

This work was supported by the Norwegian Research Council grant: 313626 'Algorithmic Governance and Cultures of Policing: Comparative Perspectives from Norway, India, Brazil, Russia, and South Africa' and Nordforsk grant: 106245 'Critical perspectives of predictive policing'. We would like to thank the guest editors of Nordic STS Studies for their expertise and dedicated support throughout the publication process of this special issue. We are also grateful to the anonymous reviewers, whose insightful comments and constructive feedback significantly guided the revision and enhancement of our manuscript.

## Author description

Helene O. I. Gundhus is Professor and head of Department of Criminology and Sociology of Law at the University of Oslo, and Professor II at the Norwegian Police University College. Her research interests include police methods and technology, police professionalism, crime prevention and security. She has also published on issues to do with risk assessments and precautionary logics, migration control and transnational policing.

Pernille Erichsen Skjervrak is a PhD Candidate at the Centre for the study of Professions, Oslo Metropolitan University. Her research interests include crime prevention, policing, professionalism and social deviation. In her PhD project, she explores standardized procedures in person-oriented preventive policing, emphasizing the practical and interpretative work of police officers and implications for accountability.

Christin Thea Wathne is a Research Professor at Work Research Institute (AFI), Oslo Metropolitan University in Norway. Her research interests include leadership and management, New Public Management, organizational development, organizational learning, professions, social identity and working environment and mastering.

## References

Archer, A., Cawston, A., Matheson, B., & Geuskens, M. (2020). Celebrity, democracy, and epistemic power. *Perspectives on politics*, 18(1), 27-42. <https://doi.org/10.1017/S1537592719002615>

Ask, K. (2016). *Lucid work. Assemblages, domestications and co-productions of play*. [Doctoral dissertation]. Norwegian University of Science and Technology.

Ask, K. and Søraa, R. A. (2024). *Digitalization and social change: A guide in critical thinking*. CRC Press.

Bowker, G. C., & Star, S. L. (1999). *Sorting things out: Classification and its consequences*. MIT Press.

Braun, V. and Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101. <https://doi.org/10.1177/1478088706qpo630a>

Brayne, S., Rosenblat, A., & Boyd, D. (2015). *Predictive policing. Data & civil rights: A new era of policing and justice*. [https://www.datacivilrights.org/pubs/2015-1027/Predictive\\_Policing.pdf](https://www.datacivilrights.org/pubs/2015-1027/Predictive_Policing.pdf)

Chan, J., Sanders, C., Bennett Moses, L., & Blackmore, H. (2022). Datafication and the practice of intelligence production. *Big Data & Society*, 9(1), 1-13. <https://doi.org/10.1177/20539517221089310>

Clarke, A. E. (2005). *Situational analysis: Grounded theory after the postmodern turn*. Sage.

Clarke, A. E., Fries, C. and Washburn, R. (2018). *Situational analysis: Grounded theory after the interpretive turn*. Sage Publications.

Cockcroft, T. (2020). *Police occupational culture: Research and practice*. Policy Press.

Douglas, M. (2002). *Purity and danger: An analysis of concepts of pollution and taboo*. Routledge.

Ellefse, B., & Lomell, H. M. (2024). Polisiær etterretning i et historisk perspektiv. In E. B. Unneberg, P. Jansen, & O. Trønnes (Eds.), *Etterretningsanalyse i politiet*. (pp. 36-56). Universitetsforlaget.

Flyverbom, M. (2019). *The Digital prism: Transparency and managed visibilities in a datafied world*. Cambridge University Press.

Flyverbom, M. (2022). Overlit: Digital architectures of visibilities. *Organization theory*, 3(3), 1-16. <https://doi.org/10.1177/26317877221090314>

Flyverbom, M. (2024). Theorizing data analysis platforms – digital refractions and reconfigurations of pasts, presents and futures. *Information, Communication & Society*, 27(13), 2366-2380. <https://doi.org/10.1080/1369118X.2024.2320907>

Foucault, M. (1977). *Discipline and punish: The birth of the prison*. Vintage Books.

Fyfe, N. R., Gundhus, H. I., & Vrist Rønn, K. (Eds.) (2018). *Moral issues in intelligence-led policing*. Routledge.

Gillespie, T. (2014). The relevance of algorithms. In T. Gillespie, P. Boczkowski, & K. Foot (Eds.), *Media technologies: Essays on communication, materiality, and society*. (pp. 167-193). MIT Press.

Gundhus, H. I. (2013). Experience or knowledge? Perspectives on new knowledge regimes and control of police professionalism. *Policing: A Journal of Theory and Practice*, 7 (2), 178-194. <https://doi.org/10.1093/police/pas039>

Gundhus, H. O. I., Skjervrak, P. E., & Wathne, C. T. (2023). We will always be better than a spreadsheet: Intelligence logic and crime prevention in practice. *European Journal of Policing Studies*, 6(1), 27-49. <https://doi.org/10.5553/EJPS/2034760X2022001009>

Gundhus, H. O. I., Talberg, N., & Wathne, C. T. (2022). From discretion to standardization: Digitalization of the police organization. *International*

*Journal of Police Science & Management*, 24(1), 27-41.  
<https://doi.org/10.1177/14613557211036554>

Gundhus, H.O.I., Wathne, C.T. (2024). Norwegian police as a learning organization in the age of data-driven intelligence? In T.Ø. Kuldova, H.O.I. Gundhus and C.T. Wathne (Eds.) *Policing and intelligence in the global big data era*, Volume II. (pp. 129-158). Palgrave's Critical Policing Studies. Palgrave Macmillan, Cham.  
[https://doi.org/10.1007/978-3-031-68298-8\\_6](https://doi.org/10.1007/978-3-031-68298-8_6)

Hartmann, M. R., & Hartmann, R. K. (2023). Hiding practices in employee-user innovation. *Research Policy*, 52(4), 104728, 1-12.  
<https://doi.org/10.1016/j.respol.2023.104728>

Haddon, L. (2007). Roger Silverstone's legacies: Domestication. *New Media & Society*, 9(1), 25-32.  
<http://doi.org/10.1177/1461444807075201>

Helmersen, N. (2024). En etterretningsanalyseprosess for politiet. In E. B. Unneberg, P. Jansen & O. Trønnes (Eds.), *Etterretningsanalyse i politiet*. (pp. 220-232). Universitetsforlaget.

Innes, M. (2006). Policing uncertainty: Countering terror through community intelligence and democratic Policing. *The Annals of the American Academy of Political and Social Science*, 605(1), 222-241.  
<https://www.jstor.org/stable/25097806>

Jasanoff, S. (2004). *States of knowledge: The co-production of science and social order*. Routledge.

Kaufmann, M. (2023). *Making information matter: Understanding surveillance and making a difference*. Bristol University Press.

Lie, M., & Sørensen, K. H. (1996). Making technology our own? Domesticating technology into everyday life. In *Making technology our own? Domesticating technology into everyday life*. Lie, M. & Sørensen, K. H. (Eds.). (pp. 1-30). Scandinavian University Press.

Lundgaard, J. M., Flinterud, G., Bjørkelo, B. & Dahl, J. Y. (2022). Transparens og tilsløring i politiets kunnskapssystemer. *Nytt Norsk Tidsskrift*, 39(2), 111-121. doi: 10.18261/nnt.39.2.2.

Lundgaard J. M., & Gundhus, H.O.I (2024). Den digitale hviskeleken: Data, informasjon og kunnskap i etterretningsstyrт politiarbeid. In E.B. Unneberg; P.T. Jansen & O. Trønnes (Eds.) *Etterretningsanalyse i politiet*. (pp. 220-232). Universitetsforlaget.

Lupton, D. (2016). *The quantified self*. Polity Press.

Molander, A. (2016). *Discretion in the welfare state: Social rights and professional judgment*. Routledge.

National Police Directorate (2014). *Etterretningsdoktrine for politiet. Versjon 1.0*. Politidirektoratet.

National Police Directorate (2017). *Rammer og retningslinjer for etablering av nye politidistrikter*. Politidirektoratet.

National Police Directorate (2020). *Etterretningsdoktrine for politiet. Versjon 1.2*. Politidirektoratet.

The Norwegian Police (2020). *Innføringshåndbok for Kunnskapsbasert politiarbeid*. Oslo: Politiet.

Oudshoorn, N., & Pinch, T. (2007). User-technology relationships: Some recent development. In E. J. Hackett, O. Amsterdamska, M.E. Lynch, & J. Wajcman (Eds.) *The handbook of science and technology studies*. (pp. 541-565). MIT Press.

Phythian M. (2012). Policing uncertainty: Intelligence, security and risk. *Intelligence and National Security*, 27(2), 187-205.  
<https://doi.org/10.1080/02684527.2012.661642>

Pinch, T.J., & W. E. Bijker (1984). The social construction of facts and artifacts: Or how the sociology of science and the sociology of technology might benefit each other. *Social Studies of Science*, 14(3), 399-431.  
<https://doi.org/10.1177/030631284014003004>

Politisregisterforskriften (2013). *Forskrift om behandling av opplysninger i politiet og påtalemyndigheten*. (FOR 2013-09-20-1097). Lovdata.

Prop. 61 LS 2014-2015. *Endringer i politiloven mv. (trygghet i hverdagen - nærpolutireformen)*. Departementenes servicesenter.

Ratcliffe, J. H. (2016). *Intelligence-led policing*. Routledge.  
<https://doi.org/10.4324/9781315717579>

Reuss-Ianni, E. (1993). *Two cultures of policing: Street cops and management cops*. Transaction Publishers

Rønn, K. V. (2022). The multifaceted norm of objectivity in intelligence practices. *Intelligence and National Security*, 37(6), 820-834.  
<https://doi.org/10.1080/02684527.2022.2076331>

Selwyn, N., & Cumbo, B. (2024). «We've tried to keep the beast on a leash»: The domestication of Digital Classroom Surveillance. *Surveillance & Society*, 22(2), 88-103.  
<https://ojs.library.queensu.ca/index.php/surveillance-and-society/index>

Silverstone R., & Haddon, L. (1996) Design and the domestication of information and communication technologies: Technical change and everyday life. In R. Silverstone & R. Mansell (Eds.) *Communication by design: The politics of information and communication technologies*. (pp. 44-74). Oxford University Press.

Silverstone, R., Hirsch, E., & Morley, D. (1992). Information and communication technologies and the moral economy of the household. In R. Silverstone & E. Hirsch (Eds.) *Consuming technologies: Media and information in domestic spaces*. (pp. 15-32). Routledge.

Skjevrek, P. E., & Gundhus, H. O. I. (2025). From personal archives to intelligence: Visibility and ignorance in forecasting 'youth at risk'. In V. Galis, H.O.I. Gundhus & A. Vradis (Eds.) *Critical perspectives on predictive policing: Anticipating proof?* (pp. 62-83). Edward Elgar publishing.

Sørensen, K. (2006) Domestication: The enactment of technology. In T. Berker, M. Hartmann, Y. Punie and K. Ward (Eds.) *Domestication of media and technologies*. (pp. 40-61). Open University Press.

Sørensen, K. H., Aune, M., & Hatling, M. (2000). Against linearity: On the cultural appropriation of science and technology. In M. Dierkes and C. von Grote (Eds.) *Between understanding and trust. The public, science and technology*. (pp. 165-178). Routledge.

Vestby, A. (2018). Policy-making without politics: Overstating objectivity in intelligence-led policing. In N. R. Fyfe, H. O. I. Gundhus, & K. V. Rønn (Eds.) *Moral issues in intelligence-led policing*. (pp. 265-282). Routledge.  
<https://doi.org/10.4324/9781315231259-14>

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books.